AF/2700/18

TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. 0113948-023

In Re Application Of: **Levergood et al.**

Serial No.	Filing Date	Examiner	Group Art Unit
09/005,479	January 12, 1998	Patrice L. Winder	2155

Invention: **INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS**

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on

The fee for filing this Appeal Brief is: **$320.00**

☒ A check in the amount of the fee is enclosed.

☐ The Commissioner has already been authorized to charge fees in this application to a Deposit Account. A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **02-1818**
A duplicate copy of this sheet is enclosed.

Signature

Dated: **March 24, 2003**

Jeffrey H. Canfield (Reg. No. 38,404)
BELL, BOYD & LLOYD LLC
P.O. Box 1135
Chicago, Illinois 60690-1135
Telephone: (312) 807-4233

I certify that this document and fee is being deposited on 03-24-03 with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature of Person Mailing Correspondence

Robert Buccieri

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

#33
LDS
4-2-03

Appellant:	Levergood et al.	)	
Serial No.:	09/005,479	)	
Title:	INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS	)	Examiner: Patrice L. Winder
		)	Group Art Unit: 2155
Filing Date:	January 12, 1998	)	
Docket No.:	113948-023	)	

Assistant Commissioner for Patents
Washington D.C. 20231

APPELLANTS' APPEAL BRIEF

Dear Sir:

This Appeal Brief is submitted pursuant to the Notice of Appeal submitted on January 24, 2003, in the above-identified patent application.

I. REAL PARTY IN INTEREST

Divine Technology Ventures is the real party in interest of the above-identified patent application by virtue of an Assignment executed on August 14, 2002 and recorded at the United States Patent and Trademark Office on Reel 113305 Frame 0593.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge there are no pending appeals or interferences that will directly affect, have a bearing on, or that will be directly affected by, the Board's decision with respect to the above-identified Appeal.

III. STATUS OF THE CLAIMS

Claims 3, 5-26, 31-43, 49-63, 67-93, 96-98, 100-106, 108-115 are pending in the Application. A copy of the appealed claims is attached in the Appendix. Claims 3, 5-6, 13-15, 17-21, 23, 32, 35-38, 49-54, 56-63, 67-75, 77, 79-93, 101, 102, 104, 106, and 112-115 stand rejected under 35 U.S.C. §102(a) as being anticipated by Jose Kahan, a distributed authorization model for WWW, (Kahan). Claims 7-12, 22, 24-26, 31, 33-34, 39-43, 55, 76, 78, and 108-111 stand rejected under 35 U.S.C. §103 as being unpatentable over Kahan in view of U.S. Patent No. 5,347,632 to Filepp et al. A copy of the Final Office Action and the prior art on which the rejection was based are included in the Supplemental Appendix.

IV. STATUS OF THE AMENDMENTS

There are no non-entered Amendments. The last Amendment entered in the application was filed on December 28, 2001. Subsequent arguments have been filed, but no Amendment after Final was filed.

V. SUMMARY OF THE INVENTION

The present invention relates to systems and methods for processing service requests over a network from a client to a server. In general, a session identifier is generated by the server and sent to and stored on the client. Thereafter, the session identifier is appended to subsequent service requests from the client to the server.

In an alternative embodiment the session identifier maybe generated, not by the server, but by a separate authentication server. Upon receiving a request from the client that does not

include a session identifier, the server may redirect the service request to an authentication server which then generates the session identifier. The authentication server sends the session identifier to the client for storage. The client then appends the session identifier to subsequent request sent to the server, or the client is immediately redirected to the server after receiving the session identifier. The session identifier being appended to the redirected service request.

Thus, the present invention calls for a method of processing service requests from a client to a server system over a network. A first step in the new method involves forwarding a service request over the network from the client to the server. Communications between the client and the server are conducted according to the hyper-text transfer protocol (HTTP). A session identifier is sent from the server system to the client. The client then stores the session identifier for use in subsequent distinct requests to the server system. The client appends the session identifier to each of the subsequent distinct requests from the client to the server system.

An embodiment of the invention provides an information system on a network and includes means for receiving service requests from a client. The means for receiving requests also determines whether the service requests include a session identifier. Again, communications between the client and server are conducted according to the HTTP. The information system further includes means for providing a session identifier to the client. The means for supplying the session identifier may be a server which receives the service requests, or may be an independent component of the network. Storage means is provided at the client for storing a session identifier received from the means for providing a session identifier. The stored session identifier is then used in subsequent communications with the server system. The client also includes means, typically software associated with a web browser, for appending the session identifier to subsequent communications from the client to the server. Finally, the system includes means for servicing the subsequent service requests sent by the client.

An alternative method according to the present invention provides for processing service requests from a client to a server system. In this embodiment, like the others, a service request having a session identifier appended thereto is received from the client, but according to this alternative method includes the step of validating the session identifier appended to the service

request is included, as is the step of, and servicing the request only if the session identifier is valid. Finally, in an alternative embodiment the service request may be a URL call command.

VI. ISSUE

Was Kahan, A Distributed Authorization Model published before the filing date of the present application?

VII. GROUPING OF THE CLAIMS

All of the claims may be grouped together. All claims stand or fall together.

VIII. ARGUMENT

Kahan, A Distributed Authorization Method, was not published prior to the filing date of the present application. The claims pending in the present application are not unpatentable under 35 U.S.C. §102(a) over Kahan nor under 35 U.S.C. §103 over Kahan in combination with other references because Kahan was not published prior to the filing date of the present invention.

A. Applicable Law

"A person shall be entitled to a patent unless – a) the invention was…printed in a publication in this or a foreign country before the invention thereof by the Applicant for patent." 35.U.S.C. §102(a). "The date of invention is presumed to be the filing date of the [] application." Ecolochem Inc. v. Southern California Edison, 56 U.S.P.Q.2d 1065, 1072 (Fed. Cir., 2000)

"Whether information is printed, handwritten, or on microfilm, or a magnetic disc or tape etc., the one who wishes to characterize the information, in whatever form it may be, as a 'printed publication', should produce sufficient proof of its dissemination or that it has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents." in Re Wyer 210 U.S.P.Q. 790, 795 (Fed.Cir., 1981).

An electronic publication, including an online database or internet publication, is considered to be a "printed publication" within the meaning of 35 U.S.C. §102(a) and (b) provided the

publication was accessible to persons concerned with the art to which the document relates. MPEP §2128 (citing in Re Wyer Id.)

There is no case law directly establishing the date on which an electronic publication becomes effective as a "printed publication" for purposes of applying 35 U.S.C. §102(a) or (b). However, by way of analogy, the policy of the Patent And Trademark Office is that a magazine is effective as a printed publication as of the date it reached the addressee and not the date it was placed in the mail. MPEP §706.02(a) (citing Protein Foundation Inc. v. Brenner, 151 U.S.P.Q. 561 (D.D.C. 1996). Furthermore, a thesis placed in a university library may be prior art if sufficiently accessible to the public. A doctoral thesis which has been indexed and shelved in a library is sufficiently accessible to the public to constitute prior art as a printed publication. In Re Hall, 781 F.2d 897, 228 U.S.P.Q. 453 (Fed.Cir. 1986). In contrast, doctoral thesis which were shelved and indexed by index cards filed in alphabetical order by student name and stored in a shoebox in a chemistry lab are not. In Re Cronyn 890 F.2d 1158, 13 U.S.P.Q.2d 1070 (Fed. Cir. 1989). Thus, the ability to locate and access printed publications is the touchstone to determining the publication date of a printed prior art publication.

The policy of the Patent and Trademark Office is to consider internet or on-line database disclosures as being publicly available as of the date the item was publicly posted. If the publication does not include a publication date (or retrieval date), it cannot be relied upon as prior art under 35 U.S.C. §102(a) or (b). MPEP 2128.1 (Citing no authority).

B. The Examiner Has Failed To Provide Evidence That Kahan, A Distributed Authorization Method Was Published Before The Filing Date Of The Present Application

The present application is a Continuation of U.S. Serial No. 08/474,096, filed June 7, 1995, and which issued as U.S. Patent No. 5,708,780. Accordingly, the present application is entitled to the effective filing date of June 7, 1995. Since, the *Kahan* reference cited by the Examiner was not published until at least June 28, 1995, *Kahan* does not qualify as prior art under 35 U.S.C. § 102(a).

The earliest date for which there is documentary evidence that the Kahan reference was available to the public is June 28, 1995. Since this is after the June 7, 1995 filing date of the present application the Kahan reference may not be considered prior art for the purpose of rejecting the appealed claims.

The Kahan reference cited by the Examiner is a paper that was presented at the INET '95 Conference Proceedings held on June 27-30, 1995, in Honolulu, Hawaii. Attachment A is the INET '95 Conference Program which on page 6 shows that J. Kahan presented A Distributed Authorization Model for WWW on June 28, 1995. Indeed, J. Kahan's personal website, a copy of which is enclosed as Attachment B, on page 2 cites the on-line reference as "J. Kahan, A distributed authorization model for WWW, In *INET'95*, June 1995." Thus, it is clear that the paper was presented on June 28, 1995 at the INET '95 Conference and that the author of the paper cites the INET '95 Conference when referencing his own paper. However, the question remains as to whether the paper was disseminated or accessible to those persons concerned with the art to which the document relates before its presentation at the INET '95 Conference.

If one follows the hyperlink under the description of the paper on Attachment B, they are taken to a page entitled "Abstract – A Distribution Authorization Model for WWW," a copy of which is enclosed as Attachment C. Attachment C was allegedly "last updated" on August 7, 1995. If one presses the "Up" icon on Attachment C, they are taken to the "Table of Contents: INET'95 Hypermedia Proceedings," a copy of which is enclosed as Attachment D. Attachment D was also allegedly "last updated" on August 7, 1995.

Returning to Attachment C, if one presses the "Full Paper" icon, they are taken to the reference cited by the Examiner, which states that the paper was "last updated" on May 5, 1995. The Examiner relies on the "last updated" date of May 5, 1995 as being the publication date. However, there is no indication that the corresponding paper was accessible or made available to those skilled in the art on that date. In fact, there is not evidence the paper was published in any way prior to the paper's presentation at the June 28, 1995, INET '95 Conference.

If one presses the icon represented by a printer on the "Abstract" page (Attachment C), they are taken to a web page as shown in Attachment E which is a PostScript or formatted version of the reference. The document shown in Attachment E indicates, at the top of each page, that the paper was part of the INET '95 Proceedings. Thus, it is clear that the paper was presented to those skilled in the art at the INET '95 Conference Proceedings on June 28, 1995. Further, Attachments C and D, both of which indicate that they were updated as late as August 7, 1995, provide the only "gateway" to the reference cited by the Examiner. The Examiner has provided no proof that the

reference was accessible through the gateway anytime before August 7, 1995 (i.e., the last update for the pages leading to the reference).

The Examiner's assertion that the reference was published on May 5, 1995 resists solely on the "last updated" date appended to the document. But this date merely indicates the date that the author submitted his final manuscript to organizers of the conference. Applicants enclose a copy of the Author Information from the INET '95 Conference as Attachment F. The Author Information contains instructions for updating the author's paper via file transfer protocol (FTP). The "last updated" line at the top of the reference is merely a part of the HTML document which has been added to indicated the date and time at which the author submitted their last update, presumably via FTP. The "last updated" line does not indicate that the paper was disseminated or otherwise accessible to anyone over the Internet or by any other means.

The mere act of submitting the document to the conference board is not an act of publication. Rather, it is akin to an author submitting a final manuscript to a publisher. In world of traditional publishing no one would consider the act of submitting a document to a publisher as amounting to publication of the document. In fact, many documents are submitted to publishers which are never published. The touchstone for determining whether a document has been published is access to the document and the ability of those interested in the art to which the document pertains to locate the document. The fact that Kahan submitted his paper to the INET '95 conference on May 7, 1995 proves nothing as regard to whether persons interested in the art of network session identifiers would have had access to or would have been able to locate the paper as of that date.

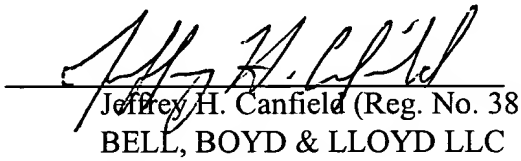
The earliest date that we have proof that the paper was available to those interested in the art was June 28, the date the paper was presented at the INET conference. Since this date is after the filing date of the present application, the Examiner has failed her burden of proving that the Kahan reference was available and accessible to person concerned with the art to which it pertains as of the filing date of the instant application. Accordingly, the Kahan reference may not be relied upon for denying the patentability of the claims pending in the application now on appeal.

All of the pending claims are rejected over *Kahan* either alone or in combination with other references. Since Kahan is not prior art with respect to the claimed invention, the final rejection of the pending claims must be reversed.

IX CONCLUSION

The reference relied on by the Examiner does not qualify as prior art against the present application. Therefore the Patent Office has failed to overcome its *prima facie* burden for rejecting the claims under 35 U.S.C. §103(a). In light of the Patent Office's failure to establish *prima facie* obviousness, Appellant respectfully submits that the rejection of pending Claims 3, 5-26, 31-43, 49-63, 67-93, 96-98, 100-106, 108-115 as being obvious an error in law and in fact and should therefore be reversed by this Board.

Respectfully submitted,



Jeffrey H. Canfield (Reg. No. 38,404)
BELL, BOYD & LLOYD LLC
P.O. Box 1135
Chicago, Illinois 60690-1135
Telephone: (312) 807-4233

ATTORNEYS FOR APPELLANTS

APPENDIX

CLAIMS:

3. (Three Times Amended) A method of processing service requests from a client to a server system through a network, said method comprising the steps of forwarding a service request from the client to the server system, wherein communications between the client and server system are according to hypertext transfer protocol;

returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent distinct requests to the server system; and

appending the stored session identifier to each of the subsequent distinct requests from the client to the server system.

5. A method as claimed in Claim 3 wherein the session identifier includes a user identifier.

6. A method as claimed in Claim 3 wherein the session identifier includes an expiration time for the session.

7. A method as claimed in Claim 3 wherein the server system records information from the session identifier in a transaction log in the server system.

8. A method as claimed in Claim 7 wherein the server system tracks the access history of sequences of service requests within a session of requests.

9. A method as claimed in Claim 8 wherein the server system tracks the access history to determine service requests leading to a purchase made within the session of requests.

10. A method as claimed in Claim 7 wherein the server system counts requests to particular services exclusive of repeated requests from a common client.

11. A method as claimed in Claim 7 wherein the server system maintains a data base relating customer information to access patterns.

12. A method as claimed in Claim 11 wherein the information includes customer demographics.

13. A method as claimed in Claim 3 wherein the server system assigns the session identifier to an initial service request to the server system.

14. A method as claimed in Claim 3 wherein the server system subjects the client to an authorization routine prior to issuing the session identifier and the session identifier is protected from forgery.

15. A method as claimed in Claim 3 wherein the server system comprises plural servers including an authentication server which provides session identifiers for service requests to multiple servers.

16. (Twice Amended) A method as claimed in Claim 15 wherein:

a client directs a service request to a first server which is to provide the requested service;

the first server checks the service request for a session identifier and only services a service request having a valid session identifier, and where the service request has no valid identifier:

the first server returns a response to the client, the response redirecting the service request from the client to the authentication server;

the authentication server subjects the client to an authorization routine and issues the session identifier to be appended to the service request to the first server;

the client forwards the service request appended with the session identifier to the first server; and

the first server recognizes the session identifier and services the service request to the client; and

the client appends the session identifier to subsequent service requests to the server system and is serviced without further authorization.

17. A method as claimed in Claim 16 wherein the session identifier includes a user identifier.

18. A method as claimed in Claim 16 wherein the session identifier includes an expiration time for the session.

19. A method as claimed in Claim 16 wherein the session identifier provides access to a protected domain to which the session has access authorization.

20. A method as claimed in Claim 19 wherein the session identifier is modified for access to a different protected domain.

21. A method as claimed in Claim 16 wherein the session identifier provides a key identifier for key management.

22. A method as claimed in Claim 16 wherein the server system records information from the session identifier in a transaction log in the server system.

23. The method of Claim 3 wherein the access rights of the client are fully contained within the session identifier.

24. (Amended) A method as claimed in Claim 3 wherein a service request is for a document and the session identifier includes a user identification, further comprising:

returning the requested document wherein the document is customized for a particular user based on the user identification of the session identifier.

25. (Amended) A method as claimed in Claim 3 wherein a service request is for a document which has been purchased by a user, the session identifier comprises an authorization identifier, and further comprising:

returning the requested document if the authorization identifier indicates that the user is authorized to access the document.

26. (Amended) A method as claimed in Claim 3 wherein a service request is for a document wherein the session identifier comprises a user identifier, and further comprising:

returning the requested document to the client; and

charging the user identified in the identifier for access to the document.

31. (Three Times Amended) The method of Claim 3, wherein at least one service request comprises a request for a document which has been purchased by a user, and wherein the session identifier comprises an authorization identifier, the method further comprising:

returning the requested document if the authorization identifier indicates that the user is authorized to access the document.

32. A method as claimed in Claim 31, wherein the authorization identifier is encoded within a session identifier which is appended to the request.

33. (Twice Amended) The method of Claim 3, wherein at least one service request comprises a request for a document, wherein the session identifier is designated by the server system, said method further comprising the steps of:

returning the requested document to the client; and

charging the user identified in the session identifier for access to the document.

34. A method as claimed in Claim 33, wherein a user identifier is encoded within a session identifier which is appended to the request.

35. (Three Times Amended) An information system on a network, comprising:

means for receiving service requests from a client and for determining whether a service request includes a session identifier, wherein communications to and from the client are according to hypertext transfer protocol;

means for providing the session identifier in response to an initial service request from the client in a session of requests;

means for storing, at the client, the session identifier for use in each communication to the server system;

means for appending the stored session identifier to each of subsequent communications from the client to the server system; and

means for servicing the subsequent service requests.

36. The information system of Claim 35 wherein access rights of the client are fully contained within the session identifier.

37. An information system as claimed in Claim 35 wherein the means for providing the session identifier is in a server system which services the requests.

38. An information system as claimed in Claim 35 further comprising an authorization routine for authorizing the client prior to issuing the session identifier and means for protecting the session identifier from forgery.

39. An information server system as claimed in Claim 35 further comprising a transaction log for recording information from the session identifier.

40. An information system as claimed in Claim 35 further comprising means for tracking access history of sequences of service requests within the session of requests.

41. An information system as claimed in Claim 35 further comprising means for counting requests to particular services exclusive of repeated requests from a common client.

42. An information system as claimed in Claim 35 further comprising a data base relating customer information to access patterns.

43. An information system as claimed in Claim 42 wherein the information includes customer demographics.

49. The method of Claim 3 wherein the session identifier is cryptographically generated.

50. (Amended) The method of Claim 3 further comprising:

returning a response to the client, the response redirecting an initial service request to an authentication server, the authentication server providing the session identifier.

51. The method of Claim 3, wherein the session identifier is appended to at least one path name in a document returned by the server system.

52. The method of Claim 51, wherein the at least one path name is in a link in the returned document.

53. The method of Claim 52 wherein the link is an absolute link.

54. The method of Claim 52 wherein the link comprises a uniform resource locator.

55. The method of Claim 51 wherein the step of appending the session identifier comprises filtering the requested document.

56. The method of Claim 51 wherein the session identifier is cryptographically generated.

57. The method of Claim 51 wherein the session identifier is directed to an accessible domain.

58. The method of Claim 51 wherein the session identifier comprises an expiration time.

59. The method of Claim 51 wherein the session identifier comprises a date.

60. The method of Claim 51 wherein the session identifier comprises a key identifier.

61. The method of Claim 51 wherein the session identifier comprises an address of the client.

62. The method of Claim 51 wherein the session identifier comprises a digital signature.

63. The method of Claim 31 wherein the authorization identifier is provided by authentication server.

67. (Amended) The method of Claim 3, wherein the session identifier is designated by the server system, further comprising the steps of:

validating, at the server system, the appended session identifier; and

returning a controlled document if the appended session identifier is valid.

68. The method of Claim 67 wherein the session identifier is cryptographically generated.

69. The method of Claim 67 wherein the session identifier is directed to an accessible domain.

70. The method of Claim 67 wherein the session identifier comprises an expiration time.

71. The method of Claim 67 wherein the session identifier comprises a date.

72. The method of Claim 67 wherein the session identifier comprises a key identifier.

73. The method of Claim 67 wherein the session identifier comprises an address of the client.

74. The method of Claim 67 wherein the session identifier comprises an unforgeable digital signature.

75. The method of Claim 67 wherein the session identifier facilitates authenticated accesses across multiple content servers.

76. The method of Claim 67 wherein the document is customized for a particular user based on a user identification of the session identifier.

77. The method of Claim 67, wherein the session identifier is appended to at least one path name in a document returned by the server system.

78. The method of Claim 77 wherein the step of appending the session identifier comprises filtering the requested document.

79. (Twice Amended) A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

forwarding a service request from the client to the server system, wherein communications between the client and server system are according to hypertext transfer protocol;

returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent communications; and

at the client, appending as part of a path name in a uniform resource locator the stored session identifier to each subsequent service request from the client to the server system within a session of requests.

80. The method of Claim 79 wherein the session identifier is cryptographically generated.

81. (Amended) The method of Claim 79 further comprising:

returning a response to the client, the response containing a locator for an authentication server, the response redirecting the first service request to the authentication server, the authentication server providing the session identifier.

82. The method of Claim 79, wherein the session identifier is appended to at least one path name in a document returned by the server system.

83. The method of Claim 82, wherein the at least one path name is in a link in the returned document.

84. The method of Claim 83 wherein the link is an absolute link.

85. The method of Claim 83 wherein the link comprises a uniform resource locator.

86. The method of Claim 82 wherein the step of appending the session identifier comprises filtering the requested document.

87. The method of Claim 82 wherein the session identifier is cryptographically generated.

88. The method of Claim 82 wherein the session identifier is directed to an accessible domain.

89. The method of Claim 82 wherein the session identifier comprises an expiration time.

90. The method of Claim 82 wherein the session identifier comprises a date.

91. The method of Claim 82 wherein the session identifier comprises a key identifier.

92. The method of Claim 82 wherein the session identifier comprises an address of the client.

93. The method of Claim 82 wherein the session identifier comprises an unforgeable digital signature.

96. The method of Claim 3, further comprising:

servicing a request; and

automatically charging a user identified by the session identifier for the service provided.

97. The method of Claim 3, wherein at least one service request comprises a purchase request, the purchase request including an associated user identifier, the method further comprising:

accessing, upon receipt of the purchase request at the server system, user information associated with the user identifier sufficient to charge to an account associated with the user, the purchase price of the product identified by the purchase request;

charging the user for the product identified by the purchase request according to the user information; and

fulfilling the purchase request based on the user information.

98. The method of Claim 97, wherein the client includes the user identifier in a session identifier appended to the purchase request.

100. The method of Claim 3, further comprising:1

under control of a client system, displaying information identifying a product; and

in response to a user selection of a hyperlink associated with a product desired to be purchased, sending a request to purchase the item along with an identifier of a purchaser of the item to a server system; and

under control of the server system, upon receiving the request, retrieving additional information previously stored for the purchaser identified by the identifier in the received request;

charging the user the purchase price of the product; and

fulfilling the request for the product.

101. The method of Claim 3, wherein the session identifier is appended by the client.

102. The method of Claim 101, wherein the session identifier is cryptographically generated.

103. The method of Claim 31, further comprising:
identifying the user from the authorization identifier; and
automatically charging the identified user for the document.

104. The method of Claim 31, wherein the document is returned electronically.

105. The method of Claim 31, wherein a physical copy of the document is sent.

106. The method of Claim 31, wherein the authorization identifier in appended to uniform resource locator.

108. (New) The method of Claim 3, wherein a service request comprises a request to purchase a product.

109. (New) The method of Claim 108, wherein the product is transmitted over the network.

110. (New) The method of Claim 109, wherein the product is a newspaper/newsletter article.

111. (New) The method of Claim 108, wherein the product is a durable product.

112. (New) A method of processing, in a server system, service requests from a client to the server system through a network, said method comprising the steps of:

receiving, from the client, a service request to which a session identifier stored at the client has been appended by the client, wherein communications between the client and server system are according to hypertext transfer protocol;

validating the session identifier appended to the service request; and servicing the service request if the appended session identifier is valid.

113. (New) The method of Claim 112, further comprising, in the server system:

receiving an initial service request from the client;

creating, responsive to the initial service request, the session identifier; and

returning the session identifier to the client for storage by the client for use in subsequent distinct requests to the server system.

114. (New) A method of processing, in a server system, uniform resource locator (URL) calls from a client to the server system through a network, said method comprising the steps of:

receiving, from the client, a URL call to which a session identifier stored at the client has been appended by the client;

validating the session identifier appended to the URL; and servicing the URL call if the appended session identifier is valid.

115. (New) The method of Claim 114, further comprising, in the server system:

receiving an initial URL call from the client;

creating, responsive to the initial URL call, the session identifier; and

returning the session identifier to the client for storage by the client for use in each URL call to the server system.

SUPPLEMENTAL APPENDIX

Exhibit A: Final Office Action (Mailed on October 24, 2002)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/005,479	01/12/1998	THOMAS MARK LEVERGOOD	OMI95-01A	2543

24573 7590 10/24/2002

BELL, BOYD & LLOYD, LLC
PO BOX 1135
CHICAGO, IL 60690-1135

EXAMINER
WINDER, PATRICE L

ART UNIT	PAPER NUMBER
2155	31

DATE MAILED: 10/24/2002

Due: 1/24/03

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/005,479	LEVERGOOD ET AL.	
	Examiner	Art Unit	
	Patrice L Winder	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2002* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,5-26,31-43,49-63,67-93,96-98,100-106 and 108-115* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,5-26,31-43,49-63,67-93,96-98,100-106 and 108-115* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. Claims 3, 5-6, 13-15, 17-21, 23, 32, 35-38, 49-54, 56-63, 67-75, 77, 79-93, 101-102, 104, 106, 112-115 are rejected under 35 U.S.C. 102(a) as being anticipated by José Kahan, A Distributed Authorization Model for WWW (hereafter referred to as Kahan).

Regarding claim 3, Kahan taught a method of processing service requests from a client to a server system through a network (abstract) comprising:

forwarding a service request from the client to the server system, wherein the communications between the client and server system are according to hypertext transport protocol (abstract);

returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent distinct requests to the server systems (Table 5); and

appending the stored session identifier to each of the subsequent distinct requests from the client to the server system (Table 5).

Regarding dependent claim 5, Kahan taught the session identifier includes a user identifier (grantee's identity, page 4).

Regarding dependent claim 6, Kahan taught the session identifier includes an expiration time for the session (Table 1).

Regarding dependent claim 13, Kahan taught the server system assigns the session identifier to an initial service request to the server system (Table 4).

Regarding dependent claim 14, Kahan taught the server system subjects the client to an authorization routine prior to issuing the session identifier (Table 4) and the session identifier is protected from forgery (Table 1).

Regarding dependent claim 15, Kahan taught plural servers including an authentication server which provides session identifier for service requests to multiple servers (Figure 1, page 3).

Regarding dependent claim 17, Kahan taught a method wherein the session identifier includes a user identifier (grantee's identity, page 4).

Regarding dependent claim 18, Kahan taught the session identifier has an expiration time includes an expiration time for the session (Table 4).

Regarding dependent claim 19, Kahan taught the session identifier provides access to a protected domain to which the session has access authorization (page 3).

Regarding dependent claim 20, Kahan taught the session identifier is modified for access to a different protected domain (access rights are generated per root document, page 6).

Regarding dependent claim 21, Kahan taught the session identifier provides a key identifier for key management (grantee identifier, page 5).

Regarding dependent claim 23, Kahan taught the access rights of the client are fully contained within the session identifier (Tables 1-3).

Regarding dependent claim 32, Kahan taught the authorization identifier is encoded within a session identifier which is appended to the requested (Table 5).

Regarding claim 35, Kahan taught an information system on a network (abstract), comprising:

means for receiving service requests from client and for determining whether a service request includes a session identifier, wherein communications to and from the clients are according to hypertext transfer protocol (Table 5);

means for providing the session identifier in response to an initial service request in a session of requests (Table 4);

means for storing, at the client, the session identifier for use in each communication to the server system (Table 5);

means for appending the stored session identifier to each of subsequent service communications from the client the server system (Table 5); and

means for servicing the subsequent service requests (Table 5).

Regarding dependent claim 36, Kahan taught the access rights of the client are fully contained within the session identifier (Table 1).

Regarding dependent claim 37, Kahan taught the means for providing the session identifier is in a server system which services the requests (Figure 1).

Regarding dependent claim 49, Kahan taught the session identifier is cryptographically generated (Table 1).

Regarding dependent claim 50, Kahan taught further comprising:

returning a response to the client, the response redirecting an initial service request to an authentication server, the authentication server providing the session identifier (Table 7).

Regarding dependent claim 51, Kahan taught wherein the session identifier is appended to at least one path name in a document returned by the server system (implementation including Sessioneer, page 13).

Regarding dependent claim 52, Kahan taught the at least one path name is a link in the returned document (implementation including Sessioneer, page 13).

Regarding dependent claim 53, Kahan taught the link is an absolute link (node links directed to document, page 13).

Regarding dependent claim 54, Kahan taught the link comprises a uniform resource locator (node links are URLs, page 13).

Regarding dependent claim 56, Kahan taught the session identifier is cryptographically generated (Table 4).

Regarding dependent claim 57, Kahan taught the session identifier is directed to an accessible domain (documents within an authorization domain, page 3).

Regarding dependent claim 58, Kahan taught the session identifier includes an expiration time for the session (Table 4).

Regarding dependent claim 59, Kahan taught the session identifier comprises a date (based on global clock, page 5).

Regarding dependent claim 60, Kahan taught the session identifier comprises a key identifier (Grantee identifier, GIA, page 5).

Regarding dependent claim 61, Kahan taught the session identifier comprises an address of the client (Grantee identifier, GIA, page 5).

Regarding dependent claim 62, Kahan taught the session identifier comprises an unforgeable digital signature (page 4).

Regarding dependent claim 63, Kahan taught the authorization identifier is provided by an authentication server (Figure 1, page 3).

Regarding dependent claim 67, Kahan taught the session identifier is designated by the server system (authorization domain, Figure 1), further comprising the steps of:

validating, at the server system, the appended session identifier (Table 5); returning a controlled document if the appended session identifier is valid (Table 5).

Regarding dependent claim 75, Kahan taught the session identifier facilitates authenticated accesses across multiple servers (Table 7).

Regarding claim 79, Kahan taught a method of processing service requests from a client to a server system through a network (abstract),

forwarding the service request from the client to the server system, wherein the communications between the client and server system are according to hypertext transfer protocol (abstract);

returning a session identifier from the server system to the client, the client storing the session identifier for use in subsequent communications (Table 4);

at the client, appending as part of a path name in a uniform resource locator the stored session identifier to each subsequent service request from the client to the service system within a session requests (Table 5).

Regarding dependent claim 101, Kahan taught the session identifier is appended by the client (Table 5).

Regarding dependent claim 102, Kahan taught the session identifier is cryptographically generated (Table 4).

Regarding dependent claim 104, Kahan taught the document is returned electronically (Table 5).

Regarding dependent claim 106, Kahan taught the authorization identifier is appended to a uniform resource locator (implementation in combination with Sessioneer, page 13).

Regarding claims 112-115, the language of claims 112-115 is substantially the same as previously rejected claims 3, 5-6, 13-15, 17-21, 23, 32, 35-38, 49-54, 56-63, 67-75, 77, 79-93. Therefore, claims 112-115 are rejected on the same rationale as claims 3, 5-6, 13-15, 17-21, 23, 32, 35-38, 49-54, 56-63, 67-75, 77, 79-93.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 7-12, 22, 24-26, 31, 33-34, 39-43, 55, 76, 78, 108-111 are rejected under 35 U.S.C. 103(a) as being unpatentable Kahan in view of Filepp et al., U.S. Patent No. 5,347,632 (hereafter referred to as Filepp).

Regarding dependent claim 7, Kahan does not specifically teach the server system recording a transaction log. However, Filepp taught a method wherein the server system records information in a transaction log in the server system (col. 93, lines 28-30).

Regarding dependent claim 8, Kahan does not specifically teach the server tracking the access history of the session. However, Filepp taught a server system that tracks the access history of sequences of service requests within a session of requests (col. 93, lines 16-24).

Regarding dependent claim 9, Kahan does not specifically teach the server system tracking the access history to determine requests leading to purchases. However, Filepp taught the server system tracking the access history to determine requests leading to purchases (within usage characteristics, col. 93, lines 28-30).

Regarding dependent claim 10, Kahan does not specifically teach a server system counting the requests. However, Filepp taught a server system counts requests

to particular services exclusive of repeated requests from a common client (col. 93, lines 28-34).

Regarding dependent claim 11, Kahan does not specifically teach a database relating customer information to access patterns. However, Filepp taught the server system maintains a database relating customer information to access patterns (col. 93, lines 28-43).

Regarding dependent 12, Kahan does not specifically teach information that includes customer demographics. However, Filepp taught wherein the information includes customer demographics (col. 9, lines 38-44).

Regarding dependent claim 22, Kahan does not specifically teach a transaction log in the server system. However, Filepp taught a method wherein the server system records information from the session identifier in a transaction log in the server system (col. 93, lines 27-47).

Regarding dependent claim 24, Kahan taught a service request is for a document (Table 5) and the session identifier includes a user identification (grantee's identity, page 4), further comprising:

returning the requested document (Table 5). Kahan does not specifically teach wherein the document is customized for a particular user based on the user identification of the session identifier. However, Filepp taught the document is customized for a particular user based on the user identification of the session identifier (col. 9, lines 27-47).

Regarding dependent claim 25, Kahan taught a service request is for a document, the session identifier comprises an authorization identifier (Table 1-3), and further comprising:

returning the requested document if the authorization identifier indicates that the user is authorized to access the document (Table 5). Kahan does not specifically teach a document which has been purchased by the user. However, Filepp taught a document which has been purchased by the user (col. 6, lines 45-51, 56-60)

Regarding dependent claim 26, Kahan taught a service request is for a document wherein the session identifier comprises a user identifier (grantee's identity, page 3, Table 1), further comprising:

returning the requested document to the client (Table 5). Kahan does not specifically teach charging the user identified in the identifier for access to the document. However, Filepp taught charging the user identified in the identifier for access to the document (col. 6, lines 57-61).

Regarding dependent claim 31, Kahan taught at least one service request comprises a document request, wherein the session identifier comprises an authorization identifier (Table 1-3), the method further comprising:

returning the requested document if the authorization identifier indicates the user is authorized to access the document (Table 5). Kahan does not specifically teach a document which has been purchased by a user. However, Filepp taught a document which has been purchased by a user (col. 6, lines 45-51, 56-60).

Regarding dependent claim 33, Kahan taught at least one service request comprises a request for a document (Table 5), wherein the session identifier is designated by the server system (Table 5), said method comprising:

returning the requested document to the client (Table 5). Kahan does not specifically teach charging the user identified in the session identifier for access to the document. However, Filepp taught charging the user identified in the session identifier for access to the document (col. 6, lines 57-61).

Regarding dependent claim 34, Kahan taught a user identifier is encoded within a session identifier which is appended to the request (grantee identity, page 4).

Regarding dependent claim 55, Kahan does not specifically teach the step of appending the session identifier comprises filtering the requested document. However, Filepp taught filtering the requested document (filtering by providing customized advertisements, col. 9, lines 38-44)

Regarding dependent claim 76, Kahan does not specifically teach the document is customized for a particular based on user identification of the session identifier. However, Filepp taught the document is customized for a particular based on user identification of the session identifier (col. 9, lines 27-47).

Regarding dependent claim 108, Kahan does not specifically teach purchasing a product. However, Filepp taught a service request is a request to purchase a product (col. 6, lines 45-51).

Regarding dependent claim 109, Filepp taught the product is transmitted over a network (col. 6, lines 45-51, 56-60).

Regarding dependent claim 110, Filepp taught the product is a newspaper/ newsletter article (col. 6, lines 45-51, 56-60).

Regarding dependent claim 111, Filepp taught the product is a durable product (col. 6, lines 56-60).

As to dependent claims, it would have been obvious to one of ordinary skill in the art at the time the invention was made that incorporating Filepp's features in Kahan's authorization system would have improved system flexibility. The motivation would have been to adapt Kahan's distributed authorization system to the individual needs of the potential users.

5. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over in view of Johnson et al., U.S. Patent No. 5,560,008 (hereafter referred to as Johnson).

Regarding dependent claim 16, Kahan does not teach another method of redirecting. However, Johnson taught a method wherein a client directs a service request to a first server which is to provide the requested service;

the first server checks the service request for a session identifier (credential id) and only services a request having a valid session identifier (credential id),

and where the service request has no valid identifier, the first server redirects the service request from the client to the authorization server (authentication agent);

the authorization server (authentication agent) subjects the client to the authorization routine and issues the session identifier (credential id) to be appended to the service request to the first server;

the client forwards the service request appended with the session identifier (credential id) to the first server;

the first server recognizes the session identifier (credential id) and services the service request to the client; and,

the client appends the session identifier (credential id) to subsequent service requests to the server system and is serviced without further authorization. Benson does not specifically teach an authorization server. However, Kahan taught a client, a first server, and an authorization server (Figure 2, col. 5). It would have been obvious to one of ordinary skill in the art at the time the invention was made that incorporating Johnson's redirecting mechanism to subsequent requests in Kahan distributed authorization system would have improved system transparency. The motivation would have been to alleviate the user from having to remember which documents require access rights and which documents do not.

6. Claims 96-98, 100, 103 and 105 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kahan in view of Dedrick, U.S. Patent No. 5,768,521 (hereafter referred to as Dedrick).

Regarding dependent claim 96, Kahan does not specifically teach how a user is charged. However, Dedrick taught servicing a request (col. 3, lines 50-56); and automatically charging a user identified by the session identifier for the service provided (col. 3, lines 60-63).

Regarding dependent claim 97, Kahan does not specifically teach a purchase request. However, Dedrick taught at least one service request comprises a purchase

request (review of the request indicates the user is not a subscriber), the purchase request including an associated user identifier (request includes information identifying whether the user is a subscriber), the method further comprising: accessing, upon receipt of the purchase request at the server system, user information associated with the user identifier sufficient to charge an account associated with the user the purchase price of the product identified by the purchase request (col. 3, lines 31-41, 60-63);

charging the user for the product identified by the purchase request according to the user information (col. 7, lines 29-35); and

fulfilling the purchase request based on the user information (col. 7, lines 35-37).

Regarding dependent claim 98, Kahan taught the client includes the user identifier in a session identifier (grantee's identity, page 3) and taught the session identifier appended to the request (Table 5). Kahan does not specifically teach the request is a purchase request. However, Dedrick taught the request is a purchase request (col. 7, lines 32-37)

Regarding dependent claim 100, Kahan does not specifically teach how a purchasing request. However, Dedrick taught under control of a client system,

displaying information identifying a product (col. 7, lines 18-23); and

in response to a user selection of a hyperlink (inherent, information distributed according to hypertext markup language, col. 4, lines 36-38) associated with a product desired to be purchased, sending a request to purchase the item along with an identifier of a purchaser of the item to a server system (id whether client is a subscriber, col. 7, lines 18-26); and

under the control of the server system, upon receiving the request, retrieving additional information previously stored for the purchaser identified by the identifier in the received request (retrieving profile containing account information, col. 3, lines 31-41, 60-63);

charging the user the purchase price of the product (metering server debits the user account, col. 7, lines 32-37); and

fulfilling the request for the product (sending information, col. 7, lines 32-37).

Regarding dependent claim 103, Kahan does not specifically teach how a user is charged. However, Dedrick taught identifying the user from the authorization identifier (identifying subscriber authorization, col. 3, lines 50-56); and

automatically charging the identified user for the document (col. 3, lines 60-63).

Regarding dependent claim 105, Kahan does not specifically teach a physical copy of the document is sent. However, Dedrick taught a physical copy of the document is sent (through the purchasing options the user is able to retrieve requested information by printing, i.e. physical copy, col. 3, lines 25-27).

Regarding claims 96, 97, 100, 103, 105, it would have been obvious to one of ordinary skill in the art at the time the invention was made that incorporating Dedrick's metering mechanisms for charging users for electronic information in Kahan's distributed authorization system would have extended the system to incorporate more mechanism to provide a better interactive environment. The motivation would have to provide a mechanism to allow a system to automatically debit and bill a user for

consuming requested electronic information from the web database (Dedrick, col. 1, lines 54-56).

Statements concerning the remaining claims

The language of claims 38-43 is substantially equivalent to the language of previously rejected claims 14, 7-8, 10-12. Therefore, claims 38-43 are rejected on the same rationale as claims 14, 7-8, 10-12, respectively.

The language of claims 68-74 is substantially equivalent to the language of previously rejected claims 56-62. Therefore, claims 68-74 are rejected on the same rationale as claims 56-62, respectively.

The language of claims 77-78 is substantially equivalent to the language of previously rejected claims 51 and 55. Therefore, claims 77-78 are rejected on the same rationale as claims 51 and 55, respectively.

The language of claims 80-93 is substantially equivalent to the language of previously rejected claims 49-62. Therefore, claims 80-93 are rejected on the same rationale as claims 49-62, respectively.

Response to Arguments

7. Applicant's arguments filed July 31, 2002, paper 328, have been fully considered but they are not persuasive.

8. Applicant argues – "Applicants disagree with the Examiner's assertion that the reference was published on May 5, 1995."

a. The paper in question was recorded as having a last update on Friday, May 5, 1995, at the World Wide Web site where posted. Thus, the date of relevance for the paper in question is May 5, 1995 in light of the paper being widely available through the Internet.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Patrice Winder whose telephone number is (703) 305-3938. The examiner can normally be reached on Monday-Friday from 10:30 AM to 7:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached on (703) 305-9648. The fax phone number(s) for this Group are after final (703) 746-7238; official (703) 746-7239 and non-official/draft (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Patrice Winder

PATRICE WINDER
PRIMARY EXAMINER

[Help] *Last update at http://inet.nttam.com: Mon Aug 7 21:47:15 1995*

INET'95 Conference Program

Conference Program : Overview

Tuesday, 27 June 1995

9:00-17:00 TUTORIALS at Sheraton Waikiki Hotel

1. Publishing with the World Wide Web
   Alan Emtage, Bunyip, Canada (bajan@bunyip.com)
2. IPng: The Next Generation Internet Protocol
   Steve Deering, Xerox PARC, USA (deering@parc.xerox.com)
3. Internet: Making the Business Case
   Gordon Howell, Internet Business Services, Scotland (gordon@ibs.co.uk)
4. Internetworking with ATM(Asynchronous Transfer Mode)
   Allison Mankin, ISI, USA (mankin@isi.edu)
5. Internet Security
   Steve Crocker, CyberCash, USA (crocker@cybercash.com)

17:00-18:00 Internet Society Open Members Meeting at Sheraton Waikiki Hotel

18:00-20:00 Opening Reception at Sheraton Waikiki Hotel

Wednesday, 28 June 1995

8:30-10:30 L1. Opening Plenary Session
Chair: Eric Schmidt (schmidt@eng.sun.com)

1. **From Conference Chair**
   Eric Schmidt (schmidt@eng.sun.com)
2. **From Governor of Hawaii**
   Benjamin J. Cayetano
3. **From Internet Society**
   Vint Cerf (cerf@isoc.org)
   Larry Landweber (lhl@cs.wisc.edu)
4. **From Program Chairs**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
   Dan Lynch (dlynch@interop.com)
5. **Note on Conference Proceedings**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
6. **Keynote Speech: The Global Telecommunication Infrastructure and the Information Society**
   Jean Jipguep, ITU (JEAN.JIPGUEP@itu.ch)

11:00-12:30 PARALLEL BREAKOUT SESSIONS
12:30-14:00--Lunch
14:00-15:30 PARALLEL BREAKOUT SESSIONS
15:30-16:00 BREAK
16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS
19:00-22:30--LUAU

Thursday, 29 June 1995

8:30-10:30 L2. INET Plenary Session
Chair: David Lassner (david@oit.hawaii.edu)

1. **Keynote Speech: The Evolution and Revolution of the Web**
   Tim Berners-Lee, W3C (timbl@w3.org)

2. **INET Panel : Network Security: Do You Know Who's Breaking in Right Now?**
   Moderator: Gage, John (Sun)
   Panelist: Patrick, John (IBM)
   Panelist: Giordano, Rose Ann (DEC)
   Panelist: Shimomura, Tsutomu (SDSC)
   Panelist: Cerf, Vint (MCI)
   Panelist: Best, Reginald (3COM)

10:30-11:00 Break
11:00-12:30 PARALLEL BREAKOUT SESSIONS
12:30-14:00 Lunch
14:00-15:30 PARALLEL BREAKOUT SESSIONS
15:30-16:00 BREAK
16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS
18:30-19:30 Cocktail Party

Friday, 30 June 1995

8:30-10:00 PARALLEL BREAKOUT SESSIONS
10:00-10:30--BREAK
10:30-12:30 L3. Closing Plenary Session
Chair: Dan Lynch (dlynch@interop.com)

1. **Keynote Speech: Economic Opportunity Along the Information Superhighway**
   Jonathan Sallet, DoC, USA
2. **Keynote Speech : Internet and Consumer Electronics: Proposed Scenario for Internet Becoming Third Media after Telephone and Television**
   Kazuhiko Nishi, ASCII, Japan (nishi@ascii.co.jp)
3. **INET'96**
   Andy Bjerring, CANARIE, Canada (bjerring@canarie.ca)
4. **Internet 1996 World Exposition**
   Carl Malamud, Internet Multicasting Service, USA (carl@radio.com)
5. **Closing Remarks**
   Eric Schmidt (schmidt@eng.sun.com)

Detailed Conference Program

Tuesday, 27 June 1995

9:00-17:00 TUTORIALS at Sheraton Waikiki Hotel

1. Publishing with the World Wide Web
   Alan Emtage, Bunyip, Canada (bajan@bunyip.com)
2. IPng: The Next Generation Internet Protocol
   Steve Deering, Xerox PARC, USA (deering@parc.xerox.com)
3. Internet: Making the Business Case
   Gordon Howell, Internet Business Services, Scotland (gordon@ibs.co.uk)
4. Internetworking with ATM(Asynchronous Transfer Mode)
   Allison Mankin, ISI, USA (mankin@isi.edu)
5. Internet Security
   Steve Crocker, CyberCash, USA (crocker@cybercash.com)

17:00-18:00 Internet Society Open Members Meeting at Sheraton Waikiki Hotel

18:00-20:00 Opening Reception at Sheraton Waikiki Hotel

Wednesday, 28 June 1995

8:30-10:30 L1. Opening Plenary Session
Chair: Eric Schmidt (schmidt@eng.sun.com)

1. **From Conference Chair**
   Eric Schmidt (schmidt@eng.sun.com)

2. **From Governor of Hawaii**
   Benjamin J. Cayetano
3. **From Internet Society**
   Vint Cerf (cerf@isoc.org)
   Larry Landweber (lhl@cs.wisc.edu)
4. **From Program Chairs**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
   Dan Lynch (dlynch@interop.com)
5. **Note on Conference Proceedings**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
6. **Keynote Speech: The Global Telecommunication Infrastructure and the Information Society**
   Jean Jipguep, ITU (JEAN.JIPGUEP@itu.ch)

11:00-12:30 PARALLEL BREAKOUT SESSIONS

A1: Information Space Environments at Kauai Room
Chair: Schatz, Bruce (schatz@csl.ncsa.uiuc.edu)

1. Maintaining Link Consistency in Distributed Hyperwebs
   Kappe, Frank (fkappe@iicm.tu-graz.ac.at)
2. Interchange of Structured Multimedia Documents Containing External Information
   Acebron, Jose Jesus (acebron@ac.upc.es)
   Delgado, Jaime (delgado@ac.upc.es)
3. Experiences with On-line access to Chemical Journals
   Kirstein, Peter (P.Kirstein@cs.ucl.ac.uk)
   Montasser-Kohsari, Goli (G.MontasserKohsari@cs.ucl.ac.uk)

D1: New Partnerships for Educational Networking at Royal Hawaiian Hotel
Chair: Rutkowski, Kathy (kmr@chaos.com)

1. Building a Commercial Internet Service for Education: Learning from One Vendor's Experience
   Perlman, Richard (rdperlm@pacbell.com)
2. Common Ground: Community Networks as Catalysts
   Klingenstein, Ken (Ken.Klingenstein@Colorado.edu)
3. Learning With the World Wide Web: Connectivity Alone Will Not Save Education
   Rose, Kimberly (rose5@applelink.apple.com)

N1: Multicasting at Molokai Room
Chair: Deering, Steve (deering@parc.xerox.com)

1. Recent Activities in the MICE Conferencing Project
   Kirstein, Peter (P.Kirstein@cs.ucl.ac.uk)
   Clayman, Stuart (S.Clayman@cs.ucl.ac.uk)
   Handley, Mark (M.Handley@cs.ucl.ac.uk)
   Sasse, Angela (A.Sasse@cs.ucl.ac.uk)
2. A Tool for Configuring Multicast Data Distribution over Global Networks
   Voigt, Robert J. (voigt@ece.nps.navy.mil)
   Barton, Robert J. (barton@ece.nps.navy.mil)
   Shukla, Shridhar B. (shukla@ece.nps.navy.mil)
3. Making the MBone Real
   Thyagarajan, Ajit (ajit@ee.udel.edu)
   Casner, Stephen (casner@isi.edu)
   Deering, Steve (deering@parc.xerox.com)

P1: GII and its Relationship to the Internet - Panel at Maui Room
Chair: Kuo, Frank (kuo@ai.sri.com)

1. GII and its Relationship to the Internet (Panel)
   Kuo, Frank (kuo@ai.sri.com)
   Kahn, Robert (rkahn@cnri.reston.va.us)
   Kumon, Shumpei (shumpei@glocom.ac.jp)
   Baser, Robert (BaserR@cp.ic.gc.ca)
   Bjerring, Andrew (bjerring@canarie.ca)

R1: Developing Countries at Honolulu Room
Chair: Lawrie, Mike (mlawrie@frd.ac.za)

1. Research and Academic Networks: The Emerging Tower of Babel
   Lerch, Irving A. (lerchi@acfcluster.nyu.edu)
2. The Sustainable Development Networking Programme: Concept and Implementation
   Zambrano, Raul (zambrano@undp.org)
   Daudpota, Isa (daudpota@sdnpk.undp.org)
3. The International Science Foundation Telecommunications Program
   Mafter, Ilya (ilya@nwu.edu)
   Shkarupin, Vyacheslav (slava@prs.isf.kiev.ua)

T1: Security at Lanai Room
Chair: Huitema, Christian (huitema@sophia.inria.fr)

1. Secure TCP -- Providing Security Functions in TCP Layer
   Tsutsumi, Toshiyuki (tutumi@ori.hitachi-sk.co.jp)
   Yamaguchi, Suguru (suguru@is.aist-nara.ac.jp)
2. Measured Interference of Security Mechanisms with Network Performance
   Claffy, K. (kc@upeksa.sdsc.edu)
   Braun, Hans-Werner (hwb@upeksa.sdsc.edu)
   Gross, Andrew (grossa@sdsc.edu)

U1: Innovative Designs for Users at Waianae Room
Chair: Foster, Jill (jill.foster@newcastle.ac.uk)

1. User-Oriented Listserv Operation: A Case Study of PHNLINK
   Kim, Sara (sarakim@u.washington.edu)
2. Virtual Museums: Enjoy the Monumentale Cemetery of Milano through the Internet
   Padula, Marco (padula@nerve.itim.mi.cnr.it)
   Celati, A.
   Palumbo, L.
   Negroni, E.
   Perucca, M.
   Rinaldi, G. Rubbia
3. Collaboratory : A Virtual Community
   Watts, Margit Misangyi (watts@uhunix.uhcc.hawaii.edu)

12:30-14:00--Lunch

14:00-15:30 PARALLEL BREAKOUT SESSIONS

A2: Low Bandwidth and Wireless Applications at Kauai Room
Chair: Gerla, Mario (gerla@cs.ucla.edu)

1. Multimedia Message Distribution in a Constrained Environment
   Wijesoma, W. S. (sardha@cse.mrt.ac.lk)
   Fernando, M. S. D. (shantha@infolabs.is.lk)
   Dias, G. V. (gihan@cse.mrt.ac.lk)
2. Extending the Reach of the Internet through Paging
   Dias, Dileeka (dileeka@infolabs.is.lk)
   Dias, Gihan (gihan@infolabs.is.lk)
   Perera, Upul
3. A Remote Robotics Laboratory on the Internet
   Cao, Y. U. (yu@cs.ucla.edu)
   Chen, T.-W. (tsuwei@cs.ucla.edu)
   Harris, M. (mharris@cs.ucla.edu)
   Kahng, A. B. (abk@cs.ucla.edu)
   Lewis, M. A. (tlewis@cs.ucla.edu)
   Stechert, A. D. (andre@cs.ucla.edu)

D2: Internetworking and Educational Reform at Royal Hawaiian Hotel
Chair: Parker, Tracy LaQuey (tparker@cisco.com)

1. Internetworking and Educational Reform: The National School Network Testbed
   Hunter, Beverly (bhunter@bbn.com)
2. A Transformation of Learning: Use of the NII for Education and Lifelong Learning
   Bracey, Bonnie (bbracey@aol.com)
3. Common Knowledge: Pittsburgh
   Carlitz, Robert D. (rdc@vms.cis.pitt.edu)

Zinga, Mario (zinga@pps.pgh.pa.us)

N2: Routing and Addressing at Molokai Room
Chair: Mankin, Allison (mankin@isi.edu)

1. The Routing Arbiter in the Post-NSFnet Service World
   Manning, Bill (bmanning@isi.edu)
2. Problems and Solutions of Dynamic Host Configuration Protocol (DHCP)
   Tominaga, Akihiro (tomy@sfc.wide.ad.jp)
   Nakamura, Osamu (osamu@sfc.wide.ad.jp)
   Teraoka, Fumio (tera@csl.sony.co.jp)
   Murai, Jun (jun@sfc.wide.ad.jp)
3. Stratum-Based Aggregation of Routing Information
   Rekhter, Yakov (yakov@watson.ibm.com)

P2: Democracy at Lanai Room
Chair: Vystavil, Martin (vystavil@savba.sk)

1. Internet: Supporting Democratic Changes in the Post-Communist Slovak Republic
   Vystavil, Martin (vystavil@savba.sk)
2. Democracy and Network Interconnectivity
   Kedzie, Christopher R. (kedzie@rand.org)
3. The Internet and Grassroots Democracy: The Telecommunications Policy Roundtable of the Northeast USA (TPR-NE)
   Klein, Hans (hkklein@mit.edu)

R2: Funding Models at Honolulu Room
Chair: Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)

1. Networking the Caribbean Region via the Virgin Islands Paradise FreeNet
   de Blanc, Peter (pdeblanc@usvi.net)
2. Turkish Internet (TR-NET) Project: Policies for Organizational Framework and Funding
   Cagiltay, Kursat (kursat@knidos.cc.metu.edu.tr)
   Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)
   Taner, Erdal (erdal@metu.edu.tr)
   Ozlu, Ufuk (ufuk@kalkan.tetm.tubitak.gov.tr)
   Cakir, Serhat (serhat@kalkan.tetm.tubitak.gov.tr)
3. REUNA: How an Academic Network can be Self-Funded
   Utreras, Florencio (futreras@reuna.cl)

T2: Internet Protocol: Next Generation at Maui Room
Chair: Hinden, Robert (hinden@ipsilon.com)

1. Internet Protocol: Next Generation (Panel)
   Hinden, Bob (hinden@ipsilon.com)
   Bradner, Scott (sob@harvard.edu)
   Deering, Steve (deering@parc.xerox.com)
   Zhang, Lixia (lixia@parc.xerox.com)

U2: Museum at Waianae Room
Chair: George, St. (stgeorge@nsf.gov)

1. Artists on the Internet
   Bishop, Ann (abishop@uiuc.edu)
   Squier, Joseph (joseph@ux1.cso.uiuc.edu)
2. Building On-Ramps to the Information Superhighway: Designing, Implementing and Using Local Museum Infrastructure
   Helfrich, Paul M. (helfrich@fi.edu)
3. Bringing Museums On Line
   Mannoni, Bruno (mannoni@culture.fr)

A3: Distributed Systems at Niihau Room
Chair: Minden, Gary (GMinden@arpa.mil)

1. A Scalable, Deployable, Directory Service Framework for the Internet
   Howes, Timothy A. (tim@umich.edu)
   Smith, Mark C. (mcs@umich.edu)
2. NetAgent: A Global Search System over Internet Resources by Distributed Agents
   Park, Taeha (taeha@nuri.net)

Chon, Kilnam (chon@cosmos.kaist.ac.kr)

3. The UNITE Project: Distributed Delivery and Contribution of Multimedia Objects over the Internet
   Deniau, Cedric (deniau@eecs.ukans.edu)
   Swink, Michael (swink@eecs.ukans.edu)
   Aust, Ron (aust@kuhub.cc.ukans.edu)
   Evans, Joe (evans@eecs.ukans.edu)
   Gauch, Susan (sgauch@tisl.ukans.edu)
   Miller, Jim (miller@eecs.ukans.edu)

15:30-16:00 BREAK

16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS

A4: Security at Kauai Room
Chair: Johns, Mike St. (stjohns@arpa.mil)

1. A Distributed Authorization Model for WWW
   Kahan,Oblatt, Jose (kahan@ccett.fr)
2. Using Public Key Technology -- Issues of Binding and Protection
   Galvin, James M. (galvin@tis.com)
   Murphy, Sandra L. (murphy@tis.com)
3. Simple Key-Management for Internet Protocol (SKIP)
   Aziz, Ashar (ashar.aziz@eng.sun.com)
   Patterson, Martin (martin.patterson@france.sun.com)
   Baehr, Geoff (geoffrey.baehr@eng.sun.com)

6/28/95

D3: New Initiatives To Support School Networking at Royal Hawaiian Hotel
Chair: Smith, Jane (jane.smith@cnidr.org)

1. Internet for Schools - the Singapore Experience
   Tan, Eng Pheng (eptan@moe.ac.sg)
2. Construct Computerized Campus to Lay the NII Foundation
   Tseng, Shian-Shyong (sstseng@cis.nctu.edu.tw)
   Lu, Ai-chin (lu@moers2.edu.tw)
   Yin, Ching-Hai (yin@moers2.edu.tw)
   Chen, Yu-Hsuan (candy@moers2.edu.tw)
3. Summary of K12 Activities in Japan
   Goto, Kunio (goto@nanzan-u.ac.jp)
   Nakayama, Masaya (nakayama@nc.u-tokyo.ac.jp)
4. Setting up a Computer Mediated Communication Network for Secondary Schools
   Cagiltay, Kursat (kursat@knidos.cc.metu.edu.tr)
   Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)
   Askar, Petek (askarp@rorqual.cc.metu.edu.tr)
5. The Educational Demands of Networking Development in Lithuania
   Reklaitis, Vytautas (vytas@pit.ktu.lt)
   Strom, Jim (j.strom@doc.mmu.ac.uk)

N3: Network Management at Molokai Room
Chair: Huizer, Erik (erik.huizer@surfnet.nl)

1. Producing Quality Factors of LAN Interconnection Services
   Valimaa, Harri (Harri.Valimaa@tele.fi)
   Honkanen, Tapani (Tapani.Honkanen@tele.fi)
2. Preventing Rather than Repairing - A New Approach in ATM Network Management
   Schuhknecht, Anja (schuhknecht@lrz-muenchen.de)
   Dreo, Gabi (dreo@lrz-muenchen.de)
3. Improved Network Management Using NMW (Network Management Worm) System
   Ohno, Hiroyuki (hohno@is.titech.ac.jp)
   Shimizu, Akihiro (akihiro@is.titech.ac.jp)
4. Object Evaluator Management Function
   Choi, Taesang (choits@cstp.umkc.edu)
   Choi, Deokjai (dchoi@cctr.umkc.edu)
   Tang, Adrian (tang@cstp.umkc.edu)

P3: Law and Fair Use at Maui Room
Chair: Civille, Richard (rciville@civicnet.org)

1. Laws of Electronic Communities and Their Roads: High Noon?
   Harter, Peter (pfh@nptn.org)
2. Non-Profit Public Access Network Services (PANS) and Local Internet Service Providers (ISPs): Complement or Conflict?
   Civille, Richard (rciville@civicnet.org)
3. The Law and the Internet : Emerging Legal Issues
   Appelman, Daniel J. (dan@hewm.com)

R3: Networks as Empowering Technology at Honolulu Room
Chair: Hahn, Saul (shahn@umd5.umd.edu)

1. Japan Window: A US-Japan Internet/WWW Collaboration for Japanese Information
   Lee, Burton H. (blee@kiku.stanford.edu)
   Goto, Atsuhiro (atsuhiro@nttam.com)
   Bayle, Michael L. (bayle@fuji.stanford.edu)
   Sakamoto, Yasuhisa (sakamoto@nttam.com)
   Thibeaux, Jeremy (thibeaux@cs.stanford.edu)
2. Friends and Partners: Building Global Community on the Internet
   Cole, Greg (gcole@solar.rtd.utk.edu)
   Bulashova, Natasha (natasha@ibpm.serpukhov.su)
3. Information-Transfer Stations for Developing Countries in Asia
   Smith, Jeff (asianet@well.sf.ca.us)
4. Building A French Virtual Community On Internet: The Example of Frognet
   Oudet, Bruno (bao@access.digex.net)

T3: Alternative Access Technologies at Lanai Room
Chair: Shimojo, Shinji (shimojo@center.osaka-u.ac.jp)

1. Mobility Support in IPv6 Based on the VIP Mechanism
   Teraoka, Fumio (tera@csl.sony.co.jp)
   Uehara, Keisuke (kei@wide.ad.jp)
2. The Internet in Developing Countries: Issues and Alternatives
   Pitke, M. V. (pitke@tifrvax.tifr.res.in)
3. A Data and Telecommunications Gateway between the Internet and ISDN
   Knight, Graham (knight@cs.ucl.ac.uk)
   Bhatti, Saleem N. (S.Bhatti@cs.ucl.ac.uk)
   Clayman, Stuart (S.Clayman@cs.ucl.ac.uk)
4. Fast Packet Technologies in the Internet Environment
   Mohta, Pushpendra (pushp@cerf.net)

U3: Public Health and Medicine at Waianae Room
Chair: Akazawa, S. (akazawa@who.ch)

1. The Global Health Network
   LaPorte, Ronald (rlaporte@vms.cis.pitt.edu)
2. NIH/NLM World Wide Web Database Projects
   Rodgers, R. P. C. (rodgers@nlm.nih.gov)
3. Hospital Information System and the Internet
   Ohe, Kazuhiko (kohe@hcc.h.u-tokyo.ac.jp)
   Kaihara, Shigekoto (kaihara-jyo@h.u-tokyo.ac.jp)
   Ishikawa, Koichi Benjamin (kishikaw@ncc.go.jp)
   Hishiki, Teruyoshi (hishiki-jyo@h.u-tokyo.ac.jp)
   Nagase, Toshiko (nagase-jyo@h.u-tokyo.ac.jp)
   Sakurai, Tunetaro (sakurai-jyo@h.u-tokyo.ac.jp)
4. The Internet and the Genome Project
   Jacobson, Dan (danj@gdb.org)

D4: Using Networks for Collaborative Learning at Niihau Room
Chair: Huston, Michele (michele.huston@anu.edu.au)

1. Slovak Academic Network (SANET) and European Schools Project (ESP) in Slovakia
   Weis, Tibor (tibor@tuzvo.sk)
   Krajnak, Julius (krajnak@tuzvo.sk)
2. Educational Projects Using Networks in Chilean Elementary Schools
   Laval, Ernesto (elaval@enlaces.ufro.cl)
   Flores, Laura (lflores@enlaces.ufro.cl)
3. Constructing Japanese K-12 Network Community: Case Study

Shintani, Takashi (shintani@glocom.ac.jp)
Uchimura, Takeshi (uchimura1@applelink.apple.com)

4. The ACTEIN Program: Bringing the Internet to Australian Schools
   Huston, Michele (michele.huston@anu.edu.au)
5. Development of WWW Services in Mexico, Toward a National Information Infrastructure
   Fernandez, Jeffry (jeff@jeff.dca.udg.mx)

19:00-22:30--LUAU

Thursday, 29 June 1995

8:30-10:30 L2. INET Plenary Session
Chair: David Lassner (david@oit.hawaii.edu)

1. **Keynote Speech: The Evolution and Revolution of the Web**
   Tim Berners-Lee, W3C (timbl@w3.org)
2. **INET Panel : Network Security: Do You Know Who's Breaking in Right Now?**
   Moderator: Gage, John (Sun)
   Panelist: Patrick, John (IBM)
   Panelist: Giordano, Rose Ann (DEC)
   Panelist: Shimomura, Tsutomu (SDSC)
   Panelist: Cerf, Vint (MCI)
   Panelist: Best, Reginald (3COM)

10:30-11:00 Break

11:00-12:30 PARALLEL BREAKOUT SESSIONS

A5: Navigating the Web at Kauai Room
Chair: Bogen, Manfred (Manfred.Bogen@gmd.de)

1. The User Interface of URLs
   Hoffman, Paul E. (phoffman@proper.com)
2. Searching Internet Resources Using IP Multicast
   Kashima, Hiroaki (kashima@csce.kyushu-u.ac.jp)
   Ishida, Yoshiki (yoshiki@cc.kyushu-u.ac.jp)
   Furukawa, Zengo (zengo@ec.kyushu-u.ac.jp)
   Ushijima, Kazuo (ushijima@csce.kyushu-u.ac.jp)
3. Document Management, Digital Libraries and the Web
   Masinter, Larry (masinter@parc.xerox.com)

C1: The Internet for Business at Molokai Room
Chair: Agoston, Tom (agoston@vnet.ibm.com)

1. Publishing Models for Internet Commerce
   O'Reilly, Tim (tim@ora.com)
2. Launching Internet Services in Asia: The Hong Kong Experience
   Wong, Pindar (pindar@hk.super.net)
3. Daiichi Advanced Home Shopping Structure on the Internet
   Matsumoto, Toshifumi (matsumoto@spin.ad.jp)
   Senoo, Yoshitaka (senoo@daiichi.co.jp)

D5: Building New Global Learning Communities at Royal Hawaiian Hotel
Chair: Maak, Laurie (lmaak@netcom.com)

1. YouthCaN
   Clements, Millard (clements@acf6.nyu.edu)
2. APICNET: A Japanese Initiative to Create a Global Classroom on the Internet
   Tsubo, Toshi (tsubo@apic.or.jp)
   Kaneko, Yoko (kaneko@apic.or.jp)
   Pavonarius, Richard (richard@apic.or.jp)
   Sekiguchi, Mikiko (mikiko@apic.or.jp)
   Matsumoto, Toshifumi (matsumoto@spin.ad.jp)
3. Creating Global Learning Communities: I*EARN's Action-Based Projects
   Brown, Kristin (krbrown@igc.apc.org)

N4: Scaling the Internet Up - Panel at Maui Room

Chair: Gross, Phil (6423401@mcimail.com)
1. Scaling the Internet Up (Panel)
   Gross, Phil (6423401@mcimail.com)
   Li, Tony
   Bradner, Scott
   Rekhter, Yakov

P4: Economics and Pricing at Niihau Room
Chair: Perez, Miguel (mperez@lascar.puc.cl)
1. Public Policies to Encourage High-Speed Residential Internet Access
   Gillett, Sharon Eisner (sharon@far.mit.edu)
2. Internet Economics: What Happens When Constituencies Collide
   Bailey, Joseph (bailey@rpcp.mit.edu)
   McKnight, Lee (mcknight@rpcp.mit.edu)
3. Pricing the Internet : A Model and a Practical Implementation.
   Perez, Miguel A. (mperez@lascar.puc.cl)

R4: Pacific at Honolulu Room
Chair: Lassner, David (david@hawaii.edu)
1. Enehana Kamepiula - Computer Telecommunication for a Hawaiian Speaking Generation
   Donaghy, Keola (keola@maui.com)
2. Self-Determination in the Information Age
   Crawford, Scott P. (exec@hawaii-nation.org)
   Crawford, Kekula P. B. (kekula@hawaii-nation.org)
3. Internet Services via PEACESAT
   Okamura, Norman (norman@elele.peacesat.hawaii.edu)
   Blake, Al (alb@ffa.gov.sb)
   Lam, Reuben (rlam@elele.peacesat.hawaii.edu)
   Mukaida, Lori (lmukaida@elele.peacesat.hawaii.edu)

U4: Enterprise Networking at Waianae Room
Chair: Weider, Chris (clw@bunyip.com)
1. Internet Affects the Corporation: Experiences from Eight Years of Connectivity
   Johnson, Suzanne M. (johnson@intel.com)
2. Internet Usage Guidelines in a Commercial Setting
   Trio, Nicholas (nrt@watson.ibm.com)
   Patrick, John (jrp@vnet.ibm.com)

T4: High Performance Networking at Lanai Room
Chair: Kim, Dae Young (dykim@comsun.chungnam.ac.kr)
1. Solutions of IPng Support for Wireless-ATM Integration
   Lu, Wai (ddke0002@utmkl.bitnet)
2. Internetworking with ATM-Based Switched Virtual Networks
   Ghane, Kamran (kamran@neda.com)
3. The Failure of Conservative Congestion Control in Large Bandwidth-Delay Product Networks
   Kim, Hyogon (hkim@dsl.cis.upenn.edu)
   Farber, David J. (farber@central.cis.upenn.edu)

12:30-14:00 Lunch

14:00-15:30 PARALLEL BREAKOUT SESSIONS

A6: Engineering the Web at Kauai Room
Chair: Berners-Lee, Tim (timbl@w3.org)
1. Supporting a URI Infrastructure by Message Broadcasting
   Freitas, Vasco (vf@uminho.pt)
   Rio, Miguel (rio@uminho.pt)
   Costa, Antonio (costa@uminho.pt)
   Macedo, Joaquim (macedo@uminho.pt)
2. Schizophrenic HTTP Server
   Barrett, Alan P. (barrett@ee.und.ac.za)
3. Intelligent Caching for WWW Objects

Wessels, Duane (wessels@colorado.edu)

D6: New Concepts of Learning at Royal Hawaiian Hotel
Chair: Perlman, Richard (rdperlm@pacbell.com)

1. MegaMath: Expanding and Connecting the Mathematics Community
   Casey, Nancy (casey931@cs.uidaho.edu)
2. The Internet and K-12 Mathematics and Science Reform
   Thomas, David (dave@mathfs.math.montana.edu)
   Stevenson, Stephanie (stevens@mail.firn.edu)
3. Science Education as a Driver of Cyberspace Technology Development
   Pea, Roy (pea@nwu.edu)
   Gomez, Louis (gomez@covis.nwu.edu)
   Edelson, Daniel (edelson@covis.nwu.edu)

N5: High Speed Networking at Molokai Room
Chair: Rekhter, Yakov (yakov@watson.ibm.com)

1. TCP/IP on Gigabit Networks
   Wilson, Anne (awilson@chernikeeff.co.uk)
2. Multimedia Experiments at the University of Pisa: From Videoconference to Random Fractals
   Giordano, Stefano (giordano@iet.unipi.it)
   Russo, Franco (russo@iet.unipi.it)
   Pierazzini, Giuseppe (peppe@pisa.infn.it)
3. Traffic Measurements in Multimedia Documents Real Time Transfer
   Lancia, Maurizio (lancia@iasi.rm.cnr.it)
   Gaibisso, Carlo (gaibisso@iasi.rm.cnr.it)
   Biondi, Vincenzo (biondi@iasi.rm.cnr.it)
   Gambosi, Giorgio (gambosi@mat.utovrm.it)
   Vitale, Maurizio (vitale@iasi.rm.cnr.it)

P5: Public Interest Regulation - Panel at Niihau Room
Chair: McClaughlin, Sean (seanm@hawaii.edu)

1. Public Interest Regulation (Panel)
   McLaughlin, Sean (seanm@Hawaii.Edu)
   Goto-Sabas, Jennifer (71532.3261@compuserve.com)
   Naito, Yukio (71532.3261@compuserve.com)
   Fukunaga, Carol (carolf@kalama.doe.hawaii.edu)
   Johanson, Cindy (cjohanson@pbs.org)
   Boutilier, Sybil (citylink@well.com)

R5: Asia at Honolulu Room
Chair: Narayan, Devendra (narayan@sut.ac.jp)

1. Connecting China Education Community to the Global Internet - The China Education and Research Network Project
   Li, Xing (xing@cernet.edu.cn)
   Wu, Jianping (jianping@cernet.edu.cn)
   Liang, Youneng (liangyn@tsinghua.edu.cn)
2. Asia Now Online
   Zoughlin, Malia (malia@uhunix.uhcc.hawaii.edu)
3. Pan Asia Networking: A Strategic Framework - Concepts, Goals, and Operations
   Wilson, Paul (pwilson@peg.apc.org)
   Hoon, Maria Ng Lee (MARIANGLEEHOON@idrc.org.sg)
   Garton, Andrew (agarton@peg.apc.org)

C2: Electronic Money at Lanai Room
Chair: Coggeshall, Bob (coggs@hongkong.cogwheel.com)

1. Using the Internet to Reduce Software Piracy
   Hauser, Ralf C. (hauser@acm.org)
2. Digital Cash and Monetary Freedom
   Matonis, Jon W. (74774.3663@compuserve.com)
3. CyberCash: Payments Systems for the Internet
   Crocker, Stephen (crocker@cybercash.com)
   Boesch, Brian (boesch@cybercash.com)
   Hart, Alden (ahart@cybercash.com)

Lum, James (jimlum@cybercash.com)

U5: Networked Information Discovery and Retrieval - Panel at Maui Room
Chair: Lynch, Cliff (clifford.lynch@ucop.edu)

1. Networked Information Discovery and Retrieval Technologies (Panel)
   Lynch, Cliff (clifford.lynch@ucop.edu)
   Michelson, Avra (avram@mitre.org)
   Preston, Cecilia (cpreston@info.berkeley.edu)
   Summerhill, Craig (craig@cni.org)

P6: Government Services at Waianae Room
Chair: Searle, Gregory (searle@tdg.uoguelph.ca)

1. Building Community Computer Networks for All Canadians: Public Ownership, Access and Communication on the Information Highway
   Searle, Gregory (searle@tdg.uoguelph.ca)
   Richardson, Don (drichard@uoguelph.ca)
   Stevenson, John (jsteven@alcor.concordia.ca)
2. The World Wide Web and Its Implications in a Democratic Society
   Doyle, Pattie (pidoyle@tdc.redstone.army.mil)
   Ross, Angela S. (aross@tdc.redstone.army.mil)
   Edwards, Rita R. (redwards@tdc.redstone.army.mil)
3. Future Prospects for NSF's International Connections Program Activities
   Goldstein, Steven N. (goldste@nsf.gov)

15:30-16:00 BREAK

16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS

A7: Infrastructure for Networked Applications - Panel at Maui Room
Chair: Leiner, Barry (bleiner@arpa.mil)

1. Infrastructure for Networked Applications (PANEL)
   Leiner, Barry (bleiner@arpa.mil)
   Huitema, Christian (huitema@sophia.inria.fr)
   Huizer, Erik (erik.huizer@surfnet.nl)
   Kummerfeld, Bob (bob@cs.su.oz.au)
   Schatz, Bruce (schatz@csl.ncsa.uiuc.edu)

D7: New Applications of Networking Technology for Education at Royal Hawaiian Hotel
Chair: Rutkowski, Kathy (kmr@chaos.com)

1. Educational Application of the Internet: International Joint Teleclass
   Aoki, Kumiko (kaoki@uhunix.uhcc.hawaii.edu)
   Goto, Kunio (goto@nanzan-u.ac.jp)
2. Net-Frog: Using the WWW to Learn about Frog Dissection and Anatomy
   Kinzie, Mable B. (Kinzie@virginia.edu)
   Larsen, Valerie A. (vl5q@virginia.edu)
   Burch, Joeseph B. (jbb@virginia.edu)
   Boker, Steven M. (boker@virginia.edu)
3. Data Exchange and Telecollaboration -- Technology in Support of New Models of Education
   Feldman, Alan (alan_feldman@terc.edu)
   Allen, Irene (irene_allen@terc.edu)
   Johnson, Lisa (lisa_johnson@terc.edu)
   Lieberman, Daniel (daniel_lieberman@terc.edu)
   Hoeven, Johan van der (johan_van_der_hoeven@terc.edu)
4. Analyzing Linkage Structure in a Course-Integrated Virtual Learning Community on the World Wide Web
   James, Leon (leon@uhunix.uhcc.hawaii.edu)
   Bogan, Kevin (bogan@uhunix.uhcc.hawaii.edu)
5. Creating Online Interactive Educational Environments: Lessons Learned from the NASA K-12 Internet Initiative
   Hodas, Steven (hodas@nsipo.nasa.gov)
   Seigel, Marc (msiegel@quest.arc.nasa.gov)

N6: High Speed Wide Area Networks at Molokai Room

Chair: Wilson, Ann (acw@chernikeeff.ac.uk)

1. Real Use of the SuperJanet High Speed Multiservice Network
   Dyer, John (John.Dyer@ukerna.ac.uk)
2. The Implementation of a High Speed Network for the DFN-Community
   Kaufmann, Peter (kaufmann@dfn.d400.de)
3. Towards a European High-Speed Backbone
   Behringer, Michael (M.H.Behringer@dante.org.uk)
4. Post-NSFNET Statistics Collection
   Claffy, K. (kc@upeksa.sdsc.edu)
   Braun, Hans-Werner (hwb@upeksa.sdsc.edu)

P7: Transborder Information Flows at Niihau Room
Chair: Peng, H.A. (mcmangph@leonis.nus.sg)

1. Internet Policy Issues in New Zealand
   Jackson, Colin (colin.jackson@comms.moc.govt.nz)
2. Censorship and the Internet: A Singapore Perspective
   Ang, Peng Hwa (mcmangph@leonis.nus.sg)
   Nadarajan, Berlinda
3. Issues in the Transborder Flow of Scientific Data
   Uhlir, Paul F. (puhlir@nas.edu)
   Alexander, Shelton S. (shel@geosc.psu.edu)

R6: Europe at Honolulu Room
Chair: Bakonyi, Peter (h25bak@ella.hu)

1. The SANET Network: Further Evolution
   Gajdos, Peter (gajdos@uakom.sk)
2. UNIBEL: Academic and Research Network of Belarus
   Kritsky, Sergei (kritsky@ok.minsk.by)
   Ivanov, Andrey (ivanov@ok.minsk.by)
   Listopad, Nikolay (listopad@cacedu.minsk.by)
3. Kiev Pilot IP Network
   Shkarupin, Viacheslav Slava (slava@prs.isf.kiev.ua)
   Demchenko, Yuri (demch@nicc.polytech.kiev.ua)
4. RUNNet - Federal University Network of Russia
   Vasilyev, Vladimir N. (vasilev@ipmo.spb.su)
   Gugel, Yuri V. (gugel@ifmo.ru)
   Kirchin, Yuri G. (kirchin@ifmo.ru)
   Robachevsky, Andrei M. (andrei@ifmo.ru)
5. Romanian National Computer Network for Research and Higher Education
   Staicut, Eugenie (estaicut@roearn.ici.ro)
   Popa, Julian (julian@roearn.ici.ro)
   Macri, George (gmacri@roearn.ici.ro)
   Toia, Adrian (atoia@roearn.ici.ro)
6. Bringing Internet to North-West of Russia -- RUSNet N/W project
   Zaborovski, Vladimir (vlad@stu.spb.su)
   Lopota, Vitaly (vlopota@stu.spb.su)
   Shemanin, Yuri (yuri@fuzzy.stu.neva.ru)
   Tarasov, Stanislav (star@stu.spb.su)

C3: Business of the Internet at Lanai Room
Chair: Takahashi, Toru (toru@tokyonet.ad.jp)

1. Tourism Promotion Using the World Wide Web
   Lennon, Martin (mlennon@chcsn1.ait.ac.nz)
2. The Internet for Small Businesses: An Enabling Infrastructure for Competitiveness
   Poon, Simpson (spoon@swin.edu.au)
   Swatman, Paula (pswatman@ponderosa.is.monash.edu.au)
3. Commercial Use of the Internet
   Levitt, Lee (levitt@process.com)

U6: Community Networking at Waianae Room
Chair: Bishop, Ann (abishop@uiuc.edu)

1. Networked Ocean Science Research and Education, Monterey Bay California
   Brutzman, Don (brutzman@nps.navy.mil)

2. Enhancing Communication and Cooperation in Human Service Delivery through the Internet
   Young, Maree
   Milosevic, Zoran (zoran@cs.uq.oz.au)
3. Potential Users and Virtual Communities in the Academic World
   Silvio, Jose (j.silvio@unesco.org)
4. Energy Utilities in the Internet and NII: Users or Providers?
   Aiken, Robert J. (aiken@es.net)
   Cavallini, John S. (cavallini@nersc.gov)
   Scott, Mary Ann (scott@er.doe.gov)

P8: Internet Privacy Guideline - Panel at Kauai Room
Chair: Rotenberg, Marc (rotenberg@epic.org)

1. Internet Privacy Guideline (Panel)
   Burrington, Bill (billburr@aol.com)
   Baser, Robert (BaserR@cp.ic.gc.ca)
   Tuerkheimer, Frank (fmtuerkh@facstaff.wisc.edu)
   Calvo, Rafael Fernandez (rfcalvo@guest2.atimdr.es)

18:30-19:30 Cocktail Party

Friday, 30 June 1995

8:30-10:00 PARALLEL BREAKOUT SESSIONS

A8: Multimedia Interface to Cyberspace at Maui Room
Chair: Kummerfeld, Bob (bob@cs.su.oz.au)

1. MMMGate - Enabling Overall Multimedia Messaging
   Bogen, Manfred (Manfred.Bogen@gmd.de)
   Krechel, Arnold (Arnold.Krechel@gmd.de)
2. Reliable Audio for Use over the Internet
   Hardman, Vicky (v.hardman@cs.ucl.ac.uk)
   Sasse, Angela (a.sasse@cs.ucl.ac.uk)
   Handley, Mark (m.handley@cs.ucl.ac.uk)
   Watson, Anna (a.watson@cs.ucl.ac.uk)
3. Use of Audio and Video on the Internet
   Muirden, Richard (richard@rmit.edu.au)

D8: Professional Development and Training at Royal Hawaiian Hotel
Chair: Huston, Michele (michele@aarnet.edu.au)

1. Teachers and Internet: Charting a Course for Success
   Buchanan, Phil (p.buchanan@mailbox.uq.oz.au)
2. Training is for Dogs: Teachers Teach; Teachers Learn
   Murray, Janet (jmurray@psg.com)
3. Blazing a Path to the Internet
   Joseph, Linda C. (ljoseph@magnus.acs.ohio-state.edu)

N7: Network Information Centers at Molokai Room
Chair: Conrad, David (davidc@keio.jp.apnic.net)

1. Financing Common Infrastructure
   Schachtner, Andreas (afs@germany.eu.net)
2. JPNIC: A Country NIC for Administrating Common Network Resources and Providing Network Information in Japan
   Hirabaru, Masaki (hi@nic.ad.jp)
   Takada, Hiroaki (hiro@nic.ad.jp)
   Nakayama, Masaya (nakayama@nic.ad.jp)
   Murai, Jun (jun@nic.ad.jp)
3. Network Skills in a Networked Information World: The Latest Tips and Tools
   Calcari, Susan (susanc@internic.net)

P9: Industrial Policy at Niihau Room
Chair: Klein, Hans (hkklein@mit.edu)

1. Measuring and Comparing the Return on Investment on Network-Related Empowerment

Ruth, Stephen (ruth@gmu.edu)
2. Surf's Up! Hawaii Attempts to Develop an Information Industry and Statewide Internetwork But Doesn't Always Catch the Right Wave
Harkness, Stephen (stephen@ptc.org)

R7: Americas at Honolulu Room
Chair: Reich, Ricardo (rreich@halcon.dpi.udec.cl)
1. Empowering Information Professionals and End Users with New Cultural Values
Ferreiro, Soledad (sferreir@abello.seci.uchile.cl)
2. Networking In Latin America and the Caribbean and the OAS/RedHUCyT Project
Hahn, Saul (shahn@umd5.umd.edu)
3. STARNET/IP : A Commercial Approach to Internet
Torres, Eduardo Jose (torrese@infomail.infonet.com)

C4: Future of Commerce on the Net at Lanai Room
Chair: Mitchell, Keith (keith@pipex.net)
1. The Emerging Internet Market
Howell, Gordon (gordon@ibs.co.uk)
Weir, George R. S. (gw@cs.strath.ac.uk)
Freeth, Tony (tony@ibs.co.uk)
2. Internet: Improving the Actual Benefit and Reducing the (Hidden) Cost
Veenis, Joop (jve@tg.nl)
3. Electronic Commerce on Internet: What Is Still Missing?
Milosevic, Zoran (zoran@cs.uq.oz.au)
Bond, Andy (bond@dstc.edu.au)

R8: Middle East/North Africa at Waianae Room
Chair: El Sherif, Hisham (hsherif@ritsec.com.eg)
1. The Communication Infrastructure and the Internet Services as a Base
Kamel, Tarek (tkamel@ritsec.com.eg)
Baki, Nashwa Abdel (nashwa@frcu.eun.eg)
2. Internet's Role in Middle-East Development: Palestinian Perspective
Zougbi, Saleem G. (saleem@bethlehem.edu)
3. Jordan's National Information System
Nusseir, Yousef (j_nic@ritsec.com.eg)
4. Networking Efforts in the Maghreb Region
Sellami, Khaled (sellami@irsit.rnrt.tn)

10:00-10:30--BREAK
10:30-12:30 L3. Closing Plenary Session
Chair: Dan Lynch (dlynch@interop.com)
1. **Keynote Speech: Economic Opportunity Along the Information Superhighway**
Jonathan Sallet, DoC, USA
2. **Keynote Speech : Internet and Consumer Electronics: Proposed Scenario for Internet Becoming Third Media after Telephone and Television**
Kazuhiko Nishi, ASCII, Japan (nishi@ascii.co.jp)
3. **INET'96**
Andy Bjerring, CANARIE, Canada (bjerring@canarie.ca)
4. **Internet 1996 World Exposition**
Carl Malamud, Internet Multicasting Service, USA (carl@radio.com)
5. **Closing Remarks**
Eric Schmidt (schmidt@eng.sun.com)

Remarks: Room Assignment

Sheraton Waikiki Hotel
Kauai, Maui, Molokai, Lanai, Niihau, Honolulu, Waianae
Royal Hawaiian Hotel
Regency

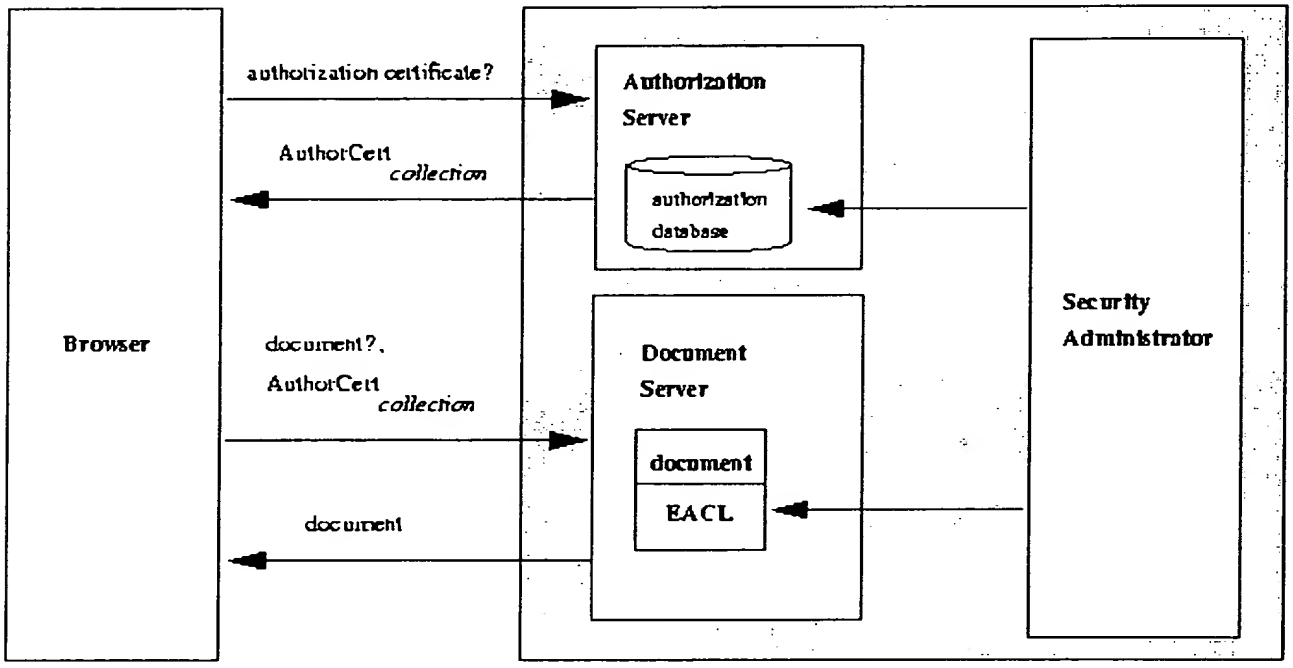
[Back to Top]

DISCLAIMER: this work represents the author's own opinions and not necessarily those of W3C or of INRIA.

WDAI

WDAI is a proposal for a simple and general infrastructure for distributed authorization on the World-Wide Web. Under WDAI, browsers and servers exchange authorization information using X.509v3-based authorization certificates.

Here's a bird's view of WDAI:



The goals of WDAI are the following:

Provide a simple and general authorization infrastructure for distributed hypertext systems

- Support of the hypertext data model (collections, document sharing),
- Offer the tools to let administrators specify their own security policies,
- Simple user administration,
- Minimize the number of data exchanges needed to authenticate and authorize a request..
- W3 compatiblity: compatible with existing protocols and browsers,

and, the most important one,

- Sensibilize more people to the problems of authorization in distributed hypertext systems.

Project history

Oct 1998: Idea for WDAI occurs while attending ApacheCon'98 (Apache developers conference)

May 1998: Paper presented at WWW8: "WDAI: a simple W3 distributed authorization infrastrcture"

Summer 1998 (expected): Tartu, a prototype implementation of WDAI using Apache, mod_ssl, open SSL, and your favorite browser.

Previous work

CAMWWW

CAMWWW is an earlier work I developed during my PhD (to be honest, CAMWWW is the name of the prototype I built, rather of the project, but it's a simple way to refer to it). I developed a non nominative capability-based access control model adapted for distributed hypermedia systems. In CAMWWW, access rights to documents are set up according to the properties of hypertext document collections. Access information is exchanged between browsers and servers using a propietary self-contained capability, inspired from the ECMA-238 standard. I built a prototype using Mosaic/PGP and the NCSA httpd server. My plan was to release it but the NSA (Never Say Anything) put pressure on the NCSA folks and made them retire Mosaic/PGP from the public distribution. Mosaic/PGP was just a patched Mosaic which had hooks for calling PGP or PEM. It didn't include either of those tools, so it was a pity it was "destroyed."

WDAI is different from CAMWWW in that it doesn't impose any security policy and that it can be used with standard SSL-enabled browsers.

Here's some of the on-line references on CAMWWW (I have a couple more, but I don't have time to put all of them here today).

- J. Kahan

  WDAI: a simple World Wide Web distributed authorization infrasutrcture

  In *Proc. WWW'9*, Computer Networks, v. 31, pp. 1599-1609, 1999.

  http://www.ww8.org/w8-papers/4d-electronic/wdai/wdai.html

- J. Kahan,
  Conception et Expérimentation d'un Modèle de Contrôle d'Accès Non Nominatif pour les Systèmes Hypermédia Répartis,
  PhD thesis, Université de Rennes I, December 1997,
  In French. ftp://ftp.irisa.fr/techreports/theses/1997/kahan.ps.gz.

- J. Kahan,
  A distributed authorization model for WWW,
  In *INET'95*, June 1995,
  http://www.isoc.org/HMP/PAPER/107/

Contributors

... are welcome!

For the moment, I'm the only one working on WDAI and I only work on it during my free time, after work hours.

Contact info

José KAHAN

W3C/INRIA, ZIRST 655, av. de l'Europe, 38330 Montbonnot Saint Martin FRANCE

jose(a)w3.org

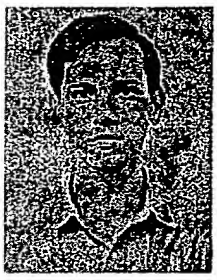
José

[Help] *Last update at http://inet.nttam.com : Mon Aug 7 21:39:55 1995*

Application Technology INET95
A4: Security

Previous Up Next
Full Paper

A Distributed Authorization Model for WWW


Kahan Oblatt, Jose (kahan@ccett.fr)

Abstract

1. PROBLEM AND MOTIVATION

The World-Wide Web (WWW) organizes information into sets of hypertext documents, where a document comprises links to contents and to other documents, rules for the document's presentation, and rules for link-traversal. Documents and contents may be stored in different servers. We use the term node to refer to either a document or a content. We refer to a set of linked documents as a presentation tree. We assume that each presentation tree has a root document.

The use of hypertext structures requires a coordinated authorization approach. Granting access to a document may require granting access to the document's linked contents. Otherwise, a browser could not correctly present the document. Moreover, granting access to a presentation tree may imply granting access to all of the documents that compose the tree. Otherwise, a user would not be able to consult a presentation tree as intended.

Existing WWW authorization schemes are based on Access-Control List (ACL) mechanisms. A document server authorizes a client's request by comparing the client's authenticated identity against the document's ACL, granting the access if the client has an entry which comprises the requested access mode. These schemes present the following drawbacks: (i) a server needs to know its potential clients; and (ii) granting or revocation of access to a document or to a presentation tree requires the modification of the ACLs associated with several nodes. Moreover, the existing schemes do not propose any infrastructure for coordinating the administration of ACLs when the documents are stored in different servers.

2. A CAPABILITY-BASED DISTRIBUTED AUTHORIZATION MODEL

We propose an authorization model which provides authorization at the document and the presentation tree levels. The model organizes document servers into authorization domains. the domain's node servers condition access to their documents to a client's presentation of appropriate capabilities. The two principal assumptions we make are: (i) a domain comprises a global clock; and (ii) a server can authenticate its clients.

The model has two phases. In an installation phase, a security administrator associates with each document a list of capabilities that correspond to the document's outgoing links to other nodes. Moreover, the security administrator generates another list of capabilities for accessing root documents and stores it in an authorization server.

In a consultation phase, the authorization server grants clients delegated capabilities for retrieving root documents. Document servers answer a client's document request with the appropriate document and a delegated version of the document's list of capabilities. The client use these capabilities to retrieve contents and other documents.

In a group extension of the model, each document is associated with an ACL whose entries correspond to the presentation trees that include the document. The authorization server now delegates to clients a group- capability granting access to a presentation tree. To access any document belonging to the presentation tree, the client just needs to present this capability.

Both the model and the group extension take into account the two approaches for document migration on the WWW, namely, the use of redirection addresses, and the use of URL-to-URN name resolvers.

Capabilities comprise attributes which protect them against their unauthorized use, modification, and forgery. Other attributes provide different capability revocation techniques.

3. UTILITY OF THE MODEL

The capability-based authorization model simplifies the security administration of clients as only the authorization server needs to know its clients.

The model allows an easy implementation of need-to-know authorization polices. Indeed, a client only obtains the capabilities necessary to consult a presentation tree and to present the tree's documents.

Moreover, we estimate that the model can be used in contexts where the client population changes at fast rates; for example, an electronic public library where a client buys access for a certain time.

4. VALIDATION OF THE MODEL

We have implemented a prototype of the capability-based authorization model and its group extension over an existing WWW system. The prototype allowed us gave us a valuable insight into how to integrate the model and its performance expectations.

[Archives]

[Help] *Last update at http://inet.nttam.com : Mon Aug 7 21:46:59 1995*

Table of Contents: INET'95 Hypermedia Proceedings

Track Index

Application Technology INET'95 [Back to Top]

A1: Information Space Environments

Chair: Schatz, Bruce (schatz@csl.ncsa.uiuc.edu)

1. Maintaining Link Consistency in Distributed Hyperwebs
   Kappe, Frank (fkappe@iicm.tu-graz.ac.at)
2. Interchange of Structured Multimedia Documents Containing External Information
   Acebron, Jose Jesus (acebron@ac.upc.es)
   Delgado, Jaime (delgado@ac.upc.es)
3. Experiences with On-line access to Chemical Journals
   Kirstein, Peter (P.Kirstein@cs.ucl.ac.uk)
   Montasser-Kohsari, Goli (G.MontasserKohsari@cs.ucl.ac.uk)

A2: Low Bandwidth and Wireless Applications

Chair: Gerla, Mario (gerla@cs.ucla.edu)

1. Multimedia Message Distribution in a Constrained Environment
   Wijesoma, W. S. (sardha@cse.mrt.ac.lk)
   Fernando, M. S. D. (shantha@infolabs.is.lk)
   Dias, G. V. (gihan@cse.mrt.ac.lk)
2. Extending the Reach of the Internet through Paging
   Dias, Dileeka (dileeka@infolabs.is.lk)
   Dias, Gihan (gihan@infolabs.is.lk)
   Perera, Upul
3. A Remote Robotics Laboratory on the Internet
   Cao, Y. U. (yu@cs.ucla.edu)
   Chen, T.-W. (tsuwei@cs.ucla.edu)
   Harris, M. (mharris@cs.ucla.edu)
   Kahng, A. B. (abk@cs.ucla.edu)
   Lewis, M. A. (tlewis@cs.ucla.edu)
   Stechert, A. D. (andre@cs.ucla.edu)

A3: Distributed Systems

Chair: Minden, Gary (GMinden@arpa.mil)

1. A Scalable, Deployable, Directory Service Framework for the Internet
   Howes, Timothy A. (tim@umich.edu)
   Smith, Mark C. (mcs@umich.edu)
2. NetAgent: A Global Search System over Internet Resources by Distributed Agents
   Park, Taeha (taeha@nuri.net)

Chon, Kilnam (chon@cosmos.kaist.ac.kr)

3. The UNITE Project: Distributed Delivery and Contribution of Multimedia Objects over the Internet
   Deniau, Cedric (deniau@eecs.ukans.edu)
   Swink, Michael (swink@eecs.ukans.edu)
   Aust, Ron (aust@kuhub.cc.ukans.edu)
   Evans, Joe (evans@eecs.ukans.edu)
   Gauch, Susan (sgauch@tisl.ukans.edu)
   Miller, Jim (miller@eecs.ukans.edu)

A4: Security

Chair: Johns, Mike St. (stjohns@arpa.mil)

1. A Distributed Authorization Model for WWW
   Kahan Oblatt, Jose (kahan@ccett.fr)
2. Using Public Key Technology -- Issues of Binding and Protection
   Galvin, James M. (galvin@tis.com)
   Murphy, Sandra L. (murphy@tis.com)
3. Simple Key-Management for Internet Protocol (SKIP)
   Aziz, Ashar (ashar.aziz@eng.sun.com)
   Patterson, Martin (martin.patterson@france.sun.com)
   Baehr, Geoff (geoffrey.baehr@eng.sun.com)

A5: Navigating the Web

Chair: Bogen, Manfred (Manfred.Bogen@gmd.de)

1. The User Interface of URLs
   Hoffman, Paul E. (phoffman@proper.com)
2. Searching Internet Resources Using IP Multicast
   Kashima, Hiroaki (kashima@csce.kyushu-u.ac.jp)
   Ishida, Yoshiki (yoshiki@cc.kyushu-u.ac.jp)
   Furukawa, Zengo (zengo@ec.kyushu-u.ac.jp)
   Ushijima, Kazuo (ushijima@csce.kyushu-u.ac.jp)
3. Document Management, Digital Libraries and the Web
   Masinter, Larry (masinter@parc.xerox.com)

A6: Engineering the Web

Chair: Berners-Lee, Tim (timbl@w3.org)

1. Supporting a URI Infrastructure by Message Broadcasting
   Freitas, Vasco (vf@uminho.pt)
   Rio, Miguel (rio@uminho.pt)
   Costa, Antonio (costa@uminho.pt)
   Macedo, Joaquim (macedo@uminho.pt)
2. Schizophrenic HTTP Server
   Barrett, Alan P. (barrett@ee.und.ac.za)
3. Intelligent Caching for WWW Objects
   Wessels, Duane (wessels@colorado.edu)

A7: Infrastructure for Networked Applications - Panel

Chair: Leiner, Barry (bleiner@arpa.mil)

1. Infrastructure for Networked Applications (PANEL)
   Leiner, Barry (bleiner@arpa.mil)
   Huitema, Christian (huitema@sophia.inria.fr)
   Huizer, Erik (erik.huizer@surfnet.nl)
   Kummerfeld, Bob (bob@cs.su.oz.au)
   Schatz, Bruce (schatz@csl.ncsa.uiuc.edu)

A8: Multimedia Interface to Cyberspace

Chair: Kummerfeld, Bob (bob@cs.su.oz.au)

1. MMMGate - Enabling Overall Multimedia Messaging
   Bogen, Manfred (Manfred.Bogen@gmd.de)
   Krechel, Arnold (Arnold.Krechel@gmd.de)
2. Reliable Audio for Use over the Internet
   Hardman, Vicky (v.hardman@cs.ucl.ac.uk)
   Sasse, Angela (a.sasse@cs.ucl.ac.uk)
   Handley, Mark (m.handley@cs.ucl.ac.uk)

Watson, Anna (a.watson@cs.ucl.ac.uk)

3. Use of Audio and Video on the Internet
   Muirden, Richard (richard@rmit.edu.au)

Commercial and Business Aspect INET'95 [Back to Top]

C1: The Internet for Business

Chair: Agoston, Tom (agoston@vnet.ibm.com)

1. Publishing Models for Internet Commerce
   O'Reilly, Tim (tim@ora.com)
2. Launching Internet Services in Asia: The Hong Kong Experience
   Wong, Pindar (pindar@hk.super.net)
3. Daiichi Advanced Home Shopping Structure on the Internet
   Matsumoto, Toshifumi (matsumoto@spin.ad.jp)
   Senoo, Yoshitaka (senoo@daiichi.co.jp)

C2: Electronic Money

Chair: Coggeshall, Bob (coggs@hongkong.cogwheel.com)

1. Using the Internet to Reduce Software Piracy
   Hauser, Ralf C. (hauser@acm.org)
2. Digital Cash and Monetary Freedom
   Matonis, Jon W. (74774.3663@compuserve.com)
3. CyberCash: Payments Systems for the Internet
   Crocker, Stephen (crocker@cybercash.com)
   Boesch, Brian (boesch@cybercash.com)
   Hart, Alden (ahart@cybercash.com)
   Lum, James (jimlum@cybercash.com)

C3: Business of the Internet

Chair: Takahashi, Toru (toru@tokyonet.ad.jp)

1. Tourism Promotion Using the World Wide Web
   Lennon, Martin (mlennon@chcsn1.ait.ac.nz)
2. The Internet for Small Businesses: An Enabling Infrastructure for Competitiveness
   Poon, Simpson (spoon@swin.edu.au)
   Swatman, Paula (pswatman@ponderosa.is.monash.edu.au)
3. Commercial Use of the Internet
   Levitt, Lee (levitt@process.com)

C4: Future of Commerce on the Net

Chair: Mitchell, Keith (keith@pipex.net)

1. The Emerging Internet Market
   Howell, Gordon (gordon@ibs.co.uk)
   Weir, George R. S. (gw@cs.strath.ac.uk)
   Freeth, Tony (tony@ibs.co.uk)
2. Internet: Improving the Actual Benefit and Reducing the (Hidden) Cost
   Veenis, Joop (jve@tg.nl)
3. Electronic Commerce on Internet: What Is Still Missing?
   Milosevic, Zoran (zoran@cs.uq.oz.au)
   Bond, Andy (bond@dstc.edu.au)

Education INET'95 [Back to Top]

D1: New Partnerships for Educational Networking

Chair: Rutkowski, Kathy (kmr@chaos.com)

1. Building a Commercial Internet Service for Education: Learning from One Vendor's Experience
   Perlman, Richard (rdperlm@pacbell.com)
2. Common Ground: Community Networks as Catalysts
   Klingenstein, Ken (Ken.Klingenstein@Colorado.edu)
3. Learning With the World Wide Web: Connectivity Alone Will Not Save Education
   Rose, Kimberly (rose5@applelink.apple.com)

D2: Internetworking and Educational Reform

Chair: Parker, Tracy LaQuey (tparker@cisco.com)

1. Internetworking and Educational Reform: The National School Network Testbed
   Hunter, Beverly (bhunter@bbn.com)
2. A Transformation of Learning: Use of the NII for Education and Lifelong Learning
   Bracey, Bonnie (bbracey@aol.com)
3. Common Knowledge: Pittsburgh
   Carlitz, Robert D. (rdc@vms.cis.pitt.edu)
   Zinga, Mario (zinga@pps.pgh.pa.us)

D3: New Initiatives To Support School Networking

Chair: Smith, Jane (jane.smith@cnidr.org)

1. Internet for Schools - the Singapore Experience
   Tan, Eng Pheng (eptan@moe.ac.sg)
2. Construct Computerized Campus to Lay the NII Foundation
   Tseng, Shian-Shyong (sstseng@cis.nctu.edu.tw)
   Lu, Ai-chin (lu@moers2.edu.tw)
   Yin, Ching-Hai (yin@moers2.edu.tw)
   Chen, Yu-Hsuan (candy@moers2.edu.tw)
3. Summary of K12 Activities in Japan
   Goto, Kunio (goto@nanzan-u.ac.jp)
   Nakayama, Masaya (nakayama@nc.u-tokyo.ac.jp)
4. Setting up a Computer Mediated Communication Network for Secondary Schools
   Cagiltay, Kursat (kursat@knidos.cc.metu.edu.tr)
   Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)
   Askar, Petek (askarp@rorqual.cc.metu.edu.tr)
5. The Educational Demands of Networking Development in Lithuania
   Reklaitis, Vytautas (vytas@pit.ktu.lt)
   Strom, Jim (j.strom@doc.mmu.ac.uk)

D4: Using Networks for Collaborative Learning

Chair: Huston, Michele (michele.huston@anu.edu.au)

1. Slovak Academic Network (SANET) and European Schools Project (ESP) in Slovakia
   Weis, Tibor (tibor@tuzvo.sk)
   Krajnak, Julius (krajnak@tuzvo.sk)
2. Educational Projects Using Networks in Chilean Elementary Schools
   Laval, Ernesto (elaval@enlaces.ufro.cl)
   Flores, Laura (lflores@enlaces.ufro.cl)
3. Constructing Japanese K-12 Network Community: Case Study
   Shintani, Takashi (shintani@glocom.ac.jp)
   Uchimura, Takeshi (uchimura1@applelink.apple.com)
4. The ACTEIN Program: Bringing the Internet to Australian Schools
   Huston, Michele (michele.huston@anu.edu.au)
5. Development of WWW Services in Mexico, Toward a National Information Infrastructure
   Fernandez, Jeffry (jeff@jeff.dca.udg.mx)

D5: Building New Global Learning Communities

Chair: Maak, Laurie (lmaak@netcom.com)

1. YouthCaN
   Clements, Millard (clements@acf6.nyu.edu)
2. APICNET: A Japanese Initiative to Create a Global Classroom on the Internet
   Tsubo, Toshi (tsubo@apic.or.jp)
   Kaneko, Yoko (kaneko@apic.or.jp)
   Pavonarius, Richard (richard@apic.or.jp)
   Sekiguchi, Mikiko (mikiko@apic.or.jp)
   Matsumoto, Toshifumi (matsumoto@spin.ad.jp)
3. Creating Global Learning Communities: I*EARN's Action-Based Projects
   Brown, Kristin (krbrown@igc.apc.org)

D6: New Concepts of Learning

Chair: Perlman, Richard (rdperlm@pacbell.com)

1. MegaMath: Expanding and Connecting the Mathematics Community
   Casey, Nancy (casey931@cs.uidaho.edu)

2. The Internet and K-12 Mathematics and Science Reform
   Thomas, David (dave@mathfs.math.montana.edu)
   Stevenson, Stephanie (stevens@mail.firn.edu)
3. Science Education as a Driver of Cyberspace Technology Development
   Pea, Roy (pea@nwu.edu)
   Gomez, Louis (gomez@covis.nwu.edu)
   Edelson, Daniel (edelson@covis.nwu.edu)

D7: New Applications of Networking Technology for Education

Chair: Rutkowski, Kathy (kmr@chaos.com)

1. Educational Application of the Internet: International Joint Teleclass
   Aoki, Kumiko (kaoki@uhunix.uhcc.hawaii.edu)
   Goto, Kunio (goto@nanzan-u.ac.jp)
2. Net-Frog: Using the WWW to Learn about Frog Dissection and Anatomy
   Kinzie, Mable B. (Kinzie@virginia.edu)
   Larsen, Valerie A. (vl5q@virginia.edu)
   Burch, Joeseph B. (jbb@virginia.edu)
   Boker, Steven M. (boker@virginia.edu)
3. Data Exchange and Telecollaboration -- Technology in Support of New Models of Education
   Feldman, Alan (alan_feldman@terc.edu)
   Allen, Irene (irene_allen@terc.edu)
   Johnson, Lisa (lisa_johnson@terc.edu)
   Lieberman, Daniel (daniel_lieberman@terc.edu)
   Hoeven, Johan van der (johan_van_der_hoeven@terc.edu)
4. Analyzing Linkage Structure in a Course-Integrated Virtual Learning Community on the World Wide Web
   James, Leon (leon@uhunix.uhcc.hawaii.edu)
   Bogan, Kevin (bogan@uhunix.uhcc.hawaii.edu)
5. Creating Online Interactive Educational Environments: Lessons Learned from the NASA K-12 Internet Initiative
   Hodas, Steven (hodas@nsipo.nasa.gov)
   Seigel, Marc (msiegel@quest.arc.nasa.gov)

D8: Professional Development and Training

Chair: Huston, Michele (michele@aarnet.edu.au)

1. Teachers and Internet: Charting a Course for Success
   Buchanan, Phil (p.buchanan@mailbox.uq.oz.au)
2. Training is for Dogs: Teachers Teach; Teachers Learn
   Murray, Janet (jmurray@psg.com)
3. Blazing a Path to the Internet
   Joseph, Linda C. (ljoseph@magnus.acs.ohio-state.edu)

Network and Application Engineering

[Back to Top]

N1: Multicasting

Chair: Deering, Steve (deering@parc.xerox.com)

1. Recent Activities in the MICE Conferencing Project
   Kirstein, Peter (P.Kirstein@cs.ucl.ac.uk)
   Clayman, Stuart (S.Clayman@cs.ucl.ac.uk)
   Handley, Mark (M.Handley@cs.ucl.ac.uk)
   Sasse, Angela (A.Sasse@cs.ucl.ac.uk)
2. A Tool for Configuring Multicast Data Distribution over Global Networks
   Voigt, Robert J. (voigt@ece.nps.navy.mil)
   Barton, Robert J. (barton@ece.nps.navy.mil)
   Shukla, Shridhar B. (shukla@ece.nps.navy.mil)
3. Making the MBone Real
   Thyagarajan, Ajit (ajit@ee.udel.edu)
   Casner, Stephen (casner@isi.edu)
   Deering, Steve (deering@parc.xerox.com)

N2: Routing and Addressing

Chair: Mankin, Allison (mankin@isi.edu)

1. The Routing Arbiter in the Post-NSFnet Service World
   Manning, Bill (bmanning@isi.edu)
2. Problems and Solutions of Dynamic Host Configuration Protocol (DHCP)
   Tominaga, Akihiro (tomy@sfc.wide.ad.jp)
   Nakamura, Osamu (osamu@sfc.wide.ad.jp)
   Teraoka, Fumio (tera@csl.sony.co.jp)
   Murai, Jun (jun@sfc.wide.ad.jp)
3. Stratum-Based Aggregation of Routing Information
   Rekhter, Yakov (yakov@watson.ibm.com)

N3: Network Management

Chair: Huizer, Erik (erik.huizer@surfnet.nl)

1. Producing Quality Factors of LAN Interconnection Services
   Valimaa, Harri (Harri.Valimaa@tele.fi)
   Honkanen, Tapani (Tapani.Honkanen@tele.fi)
2. Preventing Rather than Repairing - A New Approach in ATM Network Management
   Schuhknecht, Anja (schuhknecht@lrz-muenchen.de)
   Dreo, Gabi (dreo@lrz-muenchen.de)
3. Improved Network Management Using NMW (Network Management Worm) System
   Ohno, Hiroyuki (hohno@is.titech.ac.jp)
   Shimizu, Akihiro (akihiro@is.titech.ac.jp)
4. Object Evaluator Management Function
   Choi, Taesang (choits@cstp.umkc.edu)
   Choi, Deokjai (dchoi@cctr.umkc.edu)
   Tang, Adrian (tang@cstp.umkc.edu)

N4: Scaling the Internet Up - Panel

Chair: Gross, Phil (6423401@mcimail.com)

1. Scaling the Internet Up (Panel)
   Gross, Phil (6423401@mcimail.com)
   Li, Tony
   Bradner, Scott
   Rekhter, Yakov

N5: High Speed Networking

Chair: Rekhter, Yakov (yakov@watson.ibm.com)

1. TCP/IP on Gigabit Networks
   Wilson, Anne (awilson@chernikeeff.co.uk)
2. Multimedia Experiments at the University of Pisa: From Videoconference to Random Fractals
   Giordano, Stefano (giordano@iet.unipi.it)
   Russo, Franco (russo@iet.unipi.it)
   Pierazzini, Giuseppe (peppe@pisa.infn.it)
3. Traffic Measurements in Multimedia Documents Real Time Transfer
   Lancia, Maurizio (lancia@iasi.rm.cnr.it)
   Gaibisso, Carlo (gaibisso@iasi.rm.cnr.it)
   Biondi, Vincenzo (biondi@iasi.rm.cnr.it)
   Gambosi, Giorgio (gambosi@mat.utovrm.it)
   Vitale, Maurizio (vitale@iasi.rm.cnr.it)

N6: High Speed Wide Area Networks

Chair: Wilson, Ann (acw@chernikeeff.ac.uk)

1. Real Use of the SuperJanet High Speed Multiservice Network
   Dyer, John (John.Dyer@ukerna.ac.uk)
2. The Implementation of a High Speed Network for the DFN-Community
   Kaufmann, Peter (kaufmann@dfn.d400.de)
3. Towards a European High-Speed Backbone
   Behringer, Michael (M.H.Behringer@dante.org.uk)
4. Post-NSFNET Statistics Collection
   Claffy, K. (kc@upeksa.sdsc.edu)
   Braun, Hans-Werner (hwb@upeksa.sdsc.edu)

N7: Network Information Centers

Chair: Conrad, David (davidc@keio.jp.apnic.net)

1. Financing Common Infrastructure
   Schachtner, Andreas (afs@germany.eu.net)
2. JPNIC: A Country NIC for Administrating Common Network Resources and Providing Network Information in Japan
   Hirabaru, Masaki (hi@nic.ad.jp)
   Takada, Hiroaki (hiro@nic.ad.jp)
   Nakayama, Masaya (nakayama@nic.ad.jp)
   Murai, Jun (jun@nic.ad.jp)
3. Network Skills in a Networked Information World: The Latest Tips and Tools
   Calcari, Susan (susanc@internic.net)

Policy INET'95 [Back to Top]

P1: GII and its Relationship to the Internet - Panel
Chair: Kuo, Frank (kuo@ai.sri.com)

1. GII and its Relationship to the Internet (Panel)
   Kuo, Frank (kuo@ai.sri.com)
   Kahn, Robert (rkahn@cnri.reston.va.us)
   Kumon, Shumpei (shumpei@glocom.ac.jp)
   Baser, Robert (BaserR@cp.ic.gc.ca)
   Bjerring, Andrew (bjerring@canarie.ca)

P2: Democracy
Chair: Vystavil, Martin (vystavil@savba.sk)

1. Internet: Supporting Democratic Changes in the Post-Communist Slovak Republic
   Vystavil, Martin (vystavil@savba.sk)
2. Democracy and Network Interconnectivity
   Kedzie, Christopher R. (kedzie@rand.org)
3. The Internet and Grassroots Democracy: The Telecommunications Policy Roundtable of the Northeast USA (TPR-NE)
   Klein, Hans (hkklein@mit.edu)

P3: Law and Fair Use
Chair: Civille, Richard (rciville@civicnet.org)

1. Laws of Electronic Communities and Their Roads: High Noon?
   Harter, Peter (pfh@nptn.org)
2. Non-Profit Public Access Network Services (PANS) and Local Internet Service Providers (ISPs): Complement or Conflict?
   Civille, Richard (rciville@civicnet.org)
3. The Law and the Internet : Emerging Legal Issues
   Appelman, Daniel J. (dan@hewm.com)

P4: Economics and Pricing
Chair: Perez, Miguel (mperez@lascar.puc.cl)

1. Public Policies to Encourage High-Speed Residential Internet Access
   Gillett, Sharon Eisner (sharon@far.mit.edu)
2. Internet Economics: What Happens When Constituencies Collide
   Bailey, Joseph (bailey@rpcp.mit.edu)
   McKnight, Lee (mcknight@rpcp.mit.edu)
3. Pricing the Internet : A Model and a Practical Implementation.
   Perez, Miguel A. (mperez@lascar.puc.cl)

P5: Public Interest Regulation - Panel
Chair: McClaughlin, Sean (seanm@hawaii.edu)

1. Public Interest Regulation (Panel)
   McLaughlin, Sean (seanm@Hawaii.Edu)
   Goto-Sabas, Jennifer (71532.3261@compuserve.com)
   Naito, Yukio (71532.3261@compuserve.com)
   Fukunaga, Carol (carolf@kalama.doe.hawaii.edu)
   Johanson, Cindy (cjohanson@pbs.org)
   Boutilier, Sybil (citylink@well.com)

P6: Government Services
Chair: Searle, Gregory (searle@tdg.uoguelph.ca)

1. Building Community Computer Networks for All Canadians: Public Ownership, Access and Communication on the Information Highway
   Searle, Gregory (searle@tdg.uoguelph.ca)
   Richardson, Don (drichard@uoguelph.ca)
   Stevenson, John (jsteven@alcor.concordia.ca)
2. The World Wide Web and Its Implications in a Democratic Society
   Doyle, Pattie (pidoyle@tdc.redstone.army.mil)
   Ross, Angela S. (aross@tdc.redstone.army.mil)
   Edwards, Rita R. (redwards@tdc.redstone.army.mil)
3. Future Prospects for NSF's International Connections Program Activities
   Goldstein, Steven N. (goldste@nsf.gov)

P7: Transborder Information Flows
Chair: Peng, H.A. (mcmangph@leonis.nus.sg)

1. Internet Policy Issues in New Zealand
   Jackson, Colin (colin.jackson@comms.moc.govt.nz)
2. Censorship and the Internet: A Singapore Perspective
   Ang, Peng Hwa (mcmangph@leonis.nus.sg)
   Nadarajan, Berlinda
3. Issues in the Transborder Flow of Scientific Data
   Uhlir, Paul F. (puhlir@nas.edu)
   Alexander, Shelton S. (shel@geosc.psu.edu)

P8: Internet Privacy Guideline - Panel
Chair: Rotenberg, Marc (rotenberg@epic.org)

1. Internet Privacy Guideline (Panel)
   Burrington, Bill (billburr@aol.com)
   Baser, Robert (BaserR@cp.ic.gc.ca)
   Tuerkheimer, Frank (fmtuerkh@facstaff.wisc.edu)
   Calvo, Rafael Fernandez (rfcalvo@guest2.atimdr.es)

P9: Industrial Policy
Chair: Klein, Hans (hkklein@mit.edu)

1. Measuring and Comparing the Return on Investment on Network-Related Empowerment
   Ruth, Stephen (ruth@gmu.edu)
2. Surf's Up! Hawaii Attempts to Develop an Information Industry and Statewide Internetwork But Doesn't Always Catch the Right Wave
   Harkness, Stephen (stephen@ptc.org)

Regional INET'95 [Back to Top]

R1: Developing Countries
Chair: Lawrie, Mike (mlawrie@frd.ac.za)

1. Research and Academic Networks: The Emerging Tower of Babel
   Lerch, Irving A. (lerchi@acfcluster.nyu.edu)
2. The Sustainable Development Networking Programme: Concept and Implementation
   Zambrano, Raul (zambrano@undp.org)
   Daudpota, Isa (daudpota@sdnpk.undp.org)
3. The International Science Foundation Telecommunications Program
   Mafter, Ilya (ilya@nwu.edu)
   Shkarupin, Vyacheslav (slava@prs.isf.kiev.ua)

R2: Funding Models
Chair: Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)

1. Networking the Caribbean Region via the Virgin Islands Paradise FreeNet
   de Blanc, Peter (pdeblanc@usvi.net)
2. Turkish Internet (TR-NET) Project: Policies for Organizational Framework and Funding
   Cagiltay, Kursat (kursat@knidos.cc.metu.edu.tr)
   Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)
   Taner, Erdal (erdal@metu.edu.tr)
   Ozlu, Ufuk (ufuk@kalkan.tetm.tubitak.gov.tr)
   Cakir, Serhat (serhat@kalkan.tetm.tubitak.gov.tr)

3. REUNA: How an Academic Network can be Self-Funded
   Utreras, Florencio (futreras@reuna.cl)

R3: Networks as Empowering Technology

Chair: Hahn, Saul (shahn@umd5.umd.edu)

1. Japan Window: A US-Japan Internet/WWW Collaboration for Japanese Information
   Lee, Burton H. (blee@kiku.stanford.edu)
   Goto, Atsuhiro (atsuhiro@nttam.com)
   Bayle, Michael L. (bayle@fuji.stanford.edu)
   Sakamoto, Yasuhisa (sakamoto@nttam.com)
   Thibeaux, Jeremy (thibeaux@cs.stanford.edu)
2. Friends and Partners: Building Global Community on the Internet
   Cole, Greg (gcole@solar.rtd.utk.edu)
   Bulashova, Natasha (natasha@ibpm.serpukhov.su)
3. Information-Transfer Stations for Developing Countries in Asia
   Smith, Jeff (asianet@well.sf.ca.us)
4. Building A French Virtual Community On Internet: The Example of Frognet
   Oudet, Bruno (bao@access.digex.net)

R4: Pacific

Chair: Lassner, David (david@hawaii.edu)

1. Enehana Kamepiula - Computer Telecommunication for a Hawaiian Speaking Generation
   Donaghy, Keola (keola@maui.com)
2. Self-Determination in the Information Age
   Crawford, Scott P. (exec@hawaii-nation.org)
   Crawford, Kekula P. B. (kekula@hawaii-nation.org)
3. Internet Services via PEACESAT
   Okamura, Norman (norman@elele.peacesat.hawaii.edu)
   Blake, Al (alb@ffa.gov.sb)
   Lam, Reuben (rlam@elele.peacesat.hawaii.edu)
   Mukaida, Lori (lmukaida@elele.peacesat.hawaii.edu)

R5: Asia

Chair: Narayan, Devendra (narayan@sut.ac.jp)

1. Connecting China Education Community to the Global Internet - The China Education and Research Network Project
   Li, Xing (xing@cernet.edu.cn)
   Wu, Jianping (jianping@cernet.edu.cn)
   Liang, Youneng (liangyn@tsinghua.edu.cn)
2. Asia Now Online
   Zoughlin, Malia (malia@uhunix.uhcc.hawaii.edu)
3. Pan Asia Networking: A Strategic Framework - Concepts, Goals, and Operations
   Wilson, Paul (pwilson@peg.apc.org)
   Hoon, Maria Ng Lee (MARIANGLEEHOON@idrc.org.sg)
   Garton, Andrew (agarton@peg.apc.org)

R6: Europe

Chair: Bakonyi, Peter (h25bak@ella.hu)

1. The SANET Network: Further Evolution
   Gajdos, Peter (gajdos@uakom.sk)
2. UNIBEL: Academic and Research Network of Belarus
   Kritsky, Sergei (kritsky@ok.minsk.by)
   Ivanov, Andrey (ivanov@ok.minsk.by)
   Listopad, Nikolay (listopad@cacedu.minsk.by)
3. Kiev Pilot IP Network
   Shkarupin, Viacheslav Slava (slava@prs.isf.kiev.ua)
   Demchenko, Yuri (demch@nicc.polytech.kiev.ua)
4. RUNNet - Federal University Network of Russia
   Vasilyev, Vladimir N. (vasilev@ipmo.spb.su)
   Gugel, Yuri V. (gugel@ifmo.ru)
   Kirchin, Yuri G. (kirchin@ifmo.ru)
   Robachevsky, Andrei M. (andrei@ifmo.ru)

5. Romanian National Computer Network for Research and Higher Education
   Staicut, Eugenie (estaicut@roearn.ici.ro)
   Popa, Julian (julian@roearn.ici.ro)
   Macri, George (gmacri@roearn.ici.ro)
   Toia, Adrian (atoia@roearn.ici.ro)
6. Bringing Internet to North-West of Russia -- RUSNet N/W project
   Zaborovski, Vladimir (vlad@stu.spb.su)
   Lopota, Vitaly (vlopota@stu.spb.su)
   Shemanin, Yuri (yuri@fuzzy.stu.neva.ru)
   Tarasov, Stanislav (star@stu.spb.su)

R7: Americas

Chair: Reich, Ricardo (rreich@halcon.dpi.udec.cl)

1. Empowering Information Professionals and End Users with New Cultural Values
   Ferreiro, Soledad (sferreir@abello.seci.uchile.cl)
2. Networking In Latin America and the Caribbean and the OAS/RedHUCyT Project
   Hahn, Saul (shahn@umd5.umd.edu)
3. STARNET/IP : A Commercial Approach to Internet
   Torres, Eduardo Jose (torrese@infomail.infonet.com)

R8: Middle East/North Africa

Chair: El Sherif, Hisham (hsherif@ritsec.com.eg)

1. The Communication Infrastructure and the Internet Services as a Base
   Kamel, Tarek (tkamel@ritsec.com.eg)
   Baki, Nashwa Abdel (nashwa@frcu.eun.eg)
2. Internet's Role in Middle-East Development: Palestinian Perspective
   Zougbi, Saleem G. (saleem@bethlehem.edu)
3. Jordan's National Information System
   Nusseir, Yousef (j_nic@ritsec.com.eg)
4. Networking Efforts in the Maghreb Region
   Sellami, Khaled (sellami@irsit.rnrt.tn)

Network Technology INET'95 [Back to Top]

T1: Security

Chair: Huitema, Christian (huitema@sophia.inria.fr)

1. Secure TCP -- Providing Security Functions in TCP Layer
   Tsutsumi, Toshiyuki (tutumi@ori.hitachi-sk.co.jp)
   Yamaguchi, Suguru (suguru@is.aist-nara.ac.jp)
2. Measured Interference of Security Mechanisms with Network Performance
   Claffy, K. (kc@upeksa.sdsc.edu)
   Braun, Hans-Werner (hwb@upeksa.sdsc.edu)
   Gross, Andrew (grossa@sdsc.edu)

T2: Internet Protocol: Next Generation

Chair: Hinden, Robert (hinden@ipsilon.com)

1. Internet Protocol: Next Generation (Panel)
   Hinden, Bob (hinden@ipsilon.com)
   Bradner, Scott (sob@harvard.edu)
   Deering, Steve (deering@parc.xerox.com)
   Zhang, Lixia (lixia@parc.xerox.com)

T3: Alternative Access Technologies

Chair: Shimojo, Shinji (shimojo@center.osaka-u.ac.jp)

1. Mobility Support in IPv6 Based on the VIP Mechanism
   Teraoka, Fumio (tera@csl.sony.co.jp)
   Uehara, Keisuke (kei@wide.ad.jp)
2. The Internet in Developing Countries: Issues and Alternatives
   Pitke, M. V. (pitke@tifrvax.tifr.res.in)
3. A Data and Telecommunications Gateway between the Internet and ISDN
   Knight, Graham (knight@cs.ucl.ac.uk)
   Bhatti, Saleem N. (S.Bhatti@cs.ucl.ac.uk)

Clayman, Stuart (S.Clayman@cs.ucl.ac.uk)

4. Fast Packet Technologies in the Internet Environment
   Mohta, Pushpendra (pushp@cerf.net)

T4: High Performance Networking

Chair: Kim, Dae Young (dykim@comsun.chungnam.ac.kr)

1. Solutions of IPng Support for Wireless-ATM Integration
   Lu, Wai (ddke0002@utmkl.bitnet)
2. Internetworking with ATM-Based Switched Virtual Networks
   Ghane, Kamran (kamran@neda.com)
3. The Failure of Conservative Congestion Control in Large Bandwidth-Delay Product Networks
   Kim, Hyogon (hkim@dsl.cis.upenn.edu)
   Farber, David J. (farber@central.cis.upenn.edu)

Users INET'95 [Back to Top]

U1: Innovative Designs for Users

Chair: Foster, Jill (jill.foster@newcastle.ac.uk)

1. User-Oriented Listserv Operation: A Case Study of PHNLINK
   Kim, Sara (sarakim@u.washington.edu)
2. Virtual Museums: Enjoy the Monumentale Cemetery of Milano through the Internet
   Padula, Marco (padula@nerve.itim.mi.cnr.it)
   Celati, A.
   Palumbo, L.
   Negroni, E.
   Perucca, M.
   Rinaldi, G. Rubbia
3. Collaboratory : A Virtual Community
   Watts, Margit Misangyi (watts@uhunix.uhcc.hawaii.edu)

U2: Museum

Chair: George, St. (stgeorge@nsf.gov)

1. Artists on the Internet
   Bishop, Ann (abishop@uiuc.edu)
   Squier, Joseph (joseph@ux1.cso.uiuc.edu)
2. Building On-Ramps to the Information Superhighway: Designing, Implementing and Using Local Museum Infrastructure
   Helfrich, Paul M. (helfrich@fi.edu)
3. Bringing Museums On Line
   Mannoni, Bruno (mannoni@culture.fr)

U3: Public Health and Medicine

Chair: Akazawa, S. (akazawa@who.ch)

1. The Global Health Network
   LaPorte, Ronald (rlaporte@vms.cis.pitt.edu)
2. NIH/NLM World Wide Web Database Projects
   Rodgers, R. P. C. (rodgers@nlm.nih.gov)
3. Hospital Information System and the Internet
   Ohe, Kazuhiko (kohe@hcc.h.u-tokyo.ac.jp)
   Kaihara, Shigekoto (kaihara-jyo@h.u-tokyo.ac.jp)
   Ishikawa, Koichi Benjamin (kishikaw@ncc.go.jp)
   Hishiki, Teruyoshi (hishiki-jyo@h.u-tokyo.ac.jp)
   Nagase, Toshiko (nagase-jyo@h.u-tokyo.ac.jp)
   Sakurai, Tunetaro (sakurai-jyo@h.u-tokyo.ac.jp)
4. The Internet and the Genome Project
   Jacobson, Dan (danj@gdb.org)

U4: Enterprise Networking

Chair: Weider, Chris (clw@bunyip.com)

1. Internet Affects the Corporation: Experiences from Eight Years of Connectivity
   Johnson, Suzanne M. (johnson@intel.com)
2. Internet Usage Guidelines in a Commercial Setting

Trio, Nicholas (nrt@watson.ibm.com)
Patrick, John (jrp@vnet.ibm.com)

U5: Networked Information Discovery and Retrieval - Panel

Chair: Lynch, Cliff (clifford.lynch@ucop.edu)

1. Networked Information Discovery and Retrieval Technologies (Panel)
   Lynch, Cliff (clifford.lynch@ucop.edu)
   Michelson, Avra (avram@mitre.org)
   Preston, Cecilia (cpreston@info.berkeley.edu)
   Summerhill, Craig (craig@cni.org)

U6: Community Networking

Chair: Bishop, Ann (abishop@uiuc.edu)

1. Networked Ocean Science Research and Education, Monterey Bay California
   Brutzman, Don (brutzman@nps.navy.mil)
2. Enhancing Communication and Cooperation in Human Service Delivery through the Internet
   Young, Maree
   Milosevic, Zoran (zoran@cs.uq.oz.au)
3. Potential Users and Virtual Communities in the Academic World
   Silvio, Jose (j.silvio@unesco.org)
4. Energy Utilities in the Internet and NII: Users or Providers?
   Aiken, Robert J. (aiken@es.net)
   Cavallini, John S. (cavallini@nersc.gov)
   Scott, Mary Ann (scott@er.doe.gov)

[Back to Top]

A Distributed Authorization Model for WWW

José Kahan <kahan@ccett.fr>

Abstract

Information in WWW is organized in sets of linked hypertext documents and contents. Both documents and contents can be stored in different servers. We propose a distributed authorization model which provides coordinated authorization to related contents and documents independently of their location. Client administration is simplified as only one server needs to know its potential clients. Document and content servers make local authorization decisions using capabilities presented by their clients. The proposed model comprises sequential and non-sequential access modes. Moreover, the model supports existing WWW node migration techniques.

1 Introduction

The World-Wide Web (WWW) [6] organizes information into sets of hypertext[1] documents, where a document comprises links to media contents, links to other hypertext documents, and rules specifying the presentation of contents and the traversal of links. We refer to a set of related inter-linked documents, such as the sections of this paper, as a *presentation tree*. We refer to the entry point of a presentation tree as a *root document*. Finally, we use the term *node* to refer to either a document or a content.

WWW supports the distribution of nodes by providing node-naming structures (e.g., URLs [5]) and information retrieval protocols (e.g., HTTP [4]). By storing nodes according to their type in specialized servers, the system's overall load and capacity can be better balanced.

The use of hypertext structures requires a coordinated authorization approach. Granting access to a document should also involve granting access to the contents linked to that document. Otherwise, users would not be able to correctly perceive the document. Similarly, granting access to a presentation tree should involve granting access to all the documents that constitute the tree. Otherwise, a user would not be able to consult the presentation tree as intended.

Despite the support of distribution in WWW, little progress has been made in providing coordinated authorization under this context [24]. Existing WWW authorization approaches for distributed nodes are based on Access Control List (ACL) mechanisms [19]. These approaches require either that node servers know their potential clients or that node requests involve a consultation with an authorization server. The former approach presents a client administration problem when the client population changes at a fast rate. The latter approach presents a potential performance bottleneck as the processing of a node request depends on the availability of the authorization server.

The following sections present a distributed authorization model which supports authorization at the presentation tree and document levels for distributed documents and contents. In this model, only one server needs to know its potential clients, while node servers make local authorization decisions using capabilities presented by their clients. The model supports a sequential access mode to presentation trees. An extension to the model provides a non-sequential access mode. Section 2 gives key authorization requirements for the model. Section 3 describes the authorization model. Section 4 presents extensions to support node migration techniques. Section 5 presents a group extension which provides the non-sequential access mode. Section 6 describes our experiences in building a prototype of the model. Section 7 reviews related work in the field. The paper ends with a summary and some perspectives.

2 Authorization requirements

This section gives a brief summary (in no particular order) of the key requirements that have shaped our authorization model.

- *Coordinated authorization.* The model must support authorization at the document and presentation tree levels.
- *Distributed authorization.* To avoid a potential denial of service and to improve response time, it is important that node servers be able to take access control decisions locally, without having to consult other servers.
- *Minimization of the number of servers needing to know their potential clients.* Client

[1] In this paper, we use the terms *hypermedia* and *hypertext* interchangeably; what is said about hypertext also applies to hypermedia.

administration is simplified if few servers have to be contacted to change the status of a client.

- *Support for node sharing.* Documents and presentation trees should be able to reuse existing nodes without compromising authorization.

- *Enforcement of least privilege.* Clients should not receive more privilege than is necessary during a consultation session [20]. That is, granting access to a document should only grant additional access to the contents linked to the document; granting access to a presentation tree should only grant access to the documents that compose the tree.

- *Respect for existing WWW information retrieval protocols.* One of the reasons for the popularity of WWW is the simplicity of its protocols. The model must avoid complicating the existing protocols.

- *Backward compatibility with existing nodes.* It must be possible to control access to existing nodes without having to modify them.

- *Support for node migration.* Because of changes in computer systems and networks, nodes may need to migrate from one server to another. A user who has access rights over an object must always be able to access the object, regardless of the object's migration.

3 A capability-based authorization model

3.1 Overview

The capability-based authorization model groups node servers into *authorization domains.* Clients wishing to retrieve nodes from these servers must include appropriate capabilities [19] in their node requests.

In addition to node servers, an authorization domain comprises a *Security Administrator* (SA), responsible for the generation and installation of capabilities, as well as an *Authorization Server* (AUS), responsible for granting root document capabilities (Figure 1). Although node capabilities share the same format, we distinguish hereafter between a capability for accessing a document (Dcap) and a capability for accessing a content (Ccap) in order to explain the properties of the model.

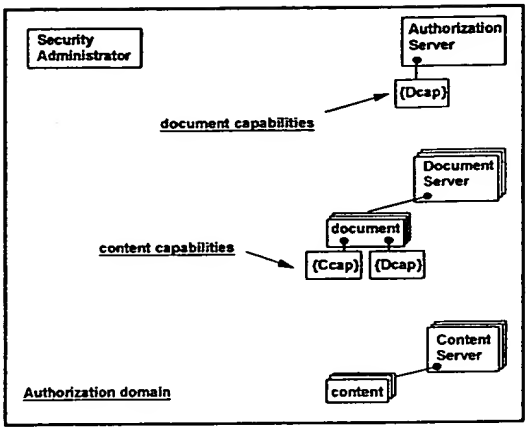


Figure 1: Authorization domain overview

During an installation phase, the SA generates for each document in the domain a list of capabilities which corresponds to the document's outgoing links to other nodes. The SA may follow a *capability association policy* to evaluate whether a capability should be associated with a link. For example, the policy could specify that only links going to children nodes should be taken into account. The SA installs these lists in the node servers that handle the corresponding documents. Moreover, the SA generates a list of capabilities that grant access to the root documents and installs it in the AUS. As the SA is the only entity that can generate new node capabilities, capability control and validation is greatly simplified. A node can be shared among different documents by associating capabilities for that node to those documents.

During a consultation phase, clients acquire nodes and capabilities. The AUS grants clients delegated capabilities for accessing root documents. Document servers grant clients documents and delegated versions of the corresponding lists of capabilities.

The AUS is the only server in the domain that needs to know its potential clients in order to authorize the granting of a capability for a root document. Node servers do not need to know their potential clients; they just require that their clients present appropriate capabilities to be able to authorize the node requests.

A capability includes attributes that allow a node server to validate it locally without needing to consult an additional server. In this way, a node request only involves one server.

The capability assignation scheme imposes a sequential order for document consultation. Section 5 describes a group extension to the model

which allows a non-sequential access to nodes.

The rest of this section describes the assumptions taken in the environment, the properties of capabilities, the message exchanges during the consultation phase, and the limitations of the model.

3.2 Environment assumptions

We assume that in an authorization domain:

- The servers of the domain can synchronize themselves with respect to a trusted, global clock [11];
- Servers can authenticate their clients;
- A node has a unique identifier in the domain; for example, a URL [5];
- Servers have a unique identity;
- A node server knows the identity of its domain's SA and AUS;
- Servers have access to a digital signature [1] mechanism; and
- A server knowing another server's identity can also verify said server's digital signature.

3.3 Properties of capabilities

This section briefly describes the format, generation, delegation, and revocation of capabilities. A previously published article [8] describes further in detail these properties.

Node identifier
Access rights
Validity period
Capability identifier
Grantor server identifier
SA identifier
SA signature

Table 1: Capability attributes

We based the format of the capabilities on that of the privilege attribute certificates (PAC) defined by the standard ECMA-138 [7]. According to this standard, a capability is generated by a *grantor* which then sends it to a *grantee*. Protection of a capability against its unauthorized propagation is achieved by including the grantee's identity inside the capability and requiring grantee authentication during the authorization process. Protection of a capability against its unauthorized use with another target is achieved by including the target's identifier inside the capability. Protection of a capability against its unauthorized modification and forgery is achieved by having the grantor server sign the capability.

Capability
Delegated access rights
Authorizator
Grantor server signature

Table 2: Delegated capability attributes

Table 1 shows the different attributes of a capability. Both the AUS and document servers grant capabilities by means of a delegation operation [23, 17, 15]. Table 2 gives the attributes of a delegated capability. A grantor server proves its right to delegate a capability by signing the delegated capability. A node server can verify this signature using the capability's `grantor server identifier` attribute. In this way, delegated capabilities can self-authenticate grantor servers.

Grantee identifier (GIA)
Validity period
Authorizator identifier
AUS identifier
AUS signature

Table 3: Authorizator attributes

A delegated capability's `authorizator` attribute is a special capability that the AUS generates when delegating a root document capability (Table 3). The authorizator's `grantee identifier` attribute (GIA) specifies the identity with which a client must authenticate itself when using the delegated capability. For instance, the value of the GIA could be an IP network address or a public key [15]. The authorizator's `validity period` attribute indicates the lifetime of a delegated capability.

The AUS is the only domain entity that can generate authorizators. Two reasons lie behind this choice. Firstly, this restriction removes the risk of having a compromised server assign unauthorized lifetimes to its delegated capabilities. Secondly, this restriction diminishes the risk of having a compromised server grant delegated capabilities to an unauthorized client.

During a session, a node server propagates the authorizator from the delegated capability associated with a request to the capabilities it will delegate. As there is only one authorizator per consultation session, the authorizator's `validity period` attribute also indicates the total time available to a client for consulting a presentation tree.

As with all capability-based systems, revocation of capabilities is a major issue. The `validity period` attributes, together with the global clock, guarantee the revocation of capabilities. Moreover, the different identifier attributes can be used to revoke capabilities before their validity expires.

3.4 Consultation phase

This phase comprises three different protocols which allow a client to retrieve a capability for a root document, a document, and a content respectively.

In the following protocols, we use the terms *Request-Node* and *Response-Node* as a shorthand notation for the actual information retrieval protocol data units used by WWW. Moreover, capabilities are distinguished from the WWW protocol data units. Finally, we show the client authentication process as a separate protocol step. The above conventions help illustrate the properties of the protocol and should not be seen as implementation guidelines.

1. Client to AUS: URL of Document + [authorization info]
2. AUS to Client: DDcap

Table 4: Root document capability retrieval

Retrieval of a root document capability. This protocol is as follows (Table 4):

1. The client first requests a root document capability from an authorization server. According to the security policy of the AUS, the client may need to include additional authorization information, such as a password or another capability. The model does not specify the type or values of this parameter.

2. In order to authorize the request, the AUS may use the client's authorization information, the URL of the document document, and any other additional security information which the AUS may have on the client. Having authorized the request, the AUS generates an authorizator and delegates the requested capability. Finally, the server returns the delegated capability to the client (we distinguish delegated capabilities with a letter "D" prefix).

1. Client to Document Server: Authentication according to the GIA
2. Client to Document Server: Request-Document + DDcap
3. Document Server to Client: Response-Document + {DDcap} + {DCcap}

Table 5: Document retrieval

Document retrieval. This protocol allows a client to retrieve a document and the document's associated list of capabilities (Table 5):

1. The client first authenticates to the document server according to the value of the GIA.

2. The client then requests the document adding the appropriate capability to the request.

3. The document server authorizes the request by verifying the integrity and validity of the delegated capability. Moreover, the server compares the authenticated client's identity against the value of the GIA. Having authorized the request, the document server uses the authorizator from the client's delegated capability to delegate the list of capabilities associated to the requested document. The server then returns the document and the delegated capabilities to the client.

1. Client to Content Server: Authentication according to the GIA
2. Client to Content Server: Request-Content + DCcap
3. Content Server to Client: Response-Content

Table 6: Content retrieval

Content retrieval. This protocol is similar to the preceding one with the exception that no delegated capabilities are returned to the client (Table 6). Indeed, contents do not have links to other nodes.

3.5 Limitations

This section briefly describes the main limitations of our authorization model.

- *Document server vulnerability.* As a document server can delegate capabilities, the compromise of this kind of server may affect other node servers.

- *Eventual lack of performance.* To validate a delegated capability, a node server has to

verify three signatures: the SA's signature of the capability, the AUS's signature of the authorizator, and the grantor server's signature of the delegated capability. When requesting a document, one must add to the validation time, the time needed to delegate the document's associated list of capabilities.

- *Regeneration of capabilities.* Whenever the validity period of a capability expires, the SA must regenerate that capability. Moreover, if the SA's signature is compromised, the SA must warn all the node servers belonging to its domain and regenerate all of the existing capabilities.

- *Bookmarks.* It is usual in WWW to copy document's URLs into local bookmark files. In the authorization model, a client can follow a bookmark link to a protected document as long as it has an appropriate capability. Once this capability expires, the bookmark link becomes useless: to obtain a new capability for the same document, the client would need to follow the tree's structure until it reaches the desired document. This limitation may be partially avoided by having the AUS grant capabilities for different documents belonging to a same presentation tree.

- *Evaluation of client consultation time.* The authorizator indicates the total time that a client has for consulting a presentation tree. However, it is not easy to give an estimation of this time: one must consider the user idle time, the workload of the node servers and the network, ... If the authorizator validity period is not correctly evaluated, a client may not be able to travel to all the nodes belonging to a presentation tree.

4 Support for node migration

This section describes how the model may support two existing node migration techniques: node migration by redirection [4], and node migration by use of Uniform Resource Names (URNs) [21, 18]. We assume that the reader is familiar with both techniques.

4.1 Node migration by redirection

In this method, a migrating node leaves a URL for its new location together with a capability for accessing it on the new server (Table 7):

1. Client to Document Server 1: Authentication according to the GIA
2. Client to Document Server 1: Request-Document + DDcap
3. Document Server 1 to Client: URL of Document + DDcap
4. Client to Document Server 2: Authentication according to the GIA
5. Client to Document Server 2: Request-Document + DDcap
6. Document Server 2 to Client: Response-Document + {DDcap} + {DCcap}

Table 7: Node redirection support

1 and 2. A client requests a protected document from document server 1.

3. Document server 1 replies with the document's new URL and a delegated capability for accessing the document at its new location.

4, 5 and 6. The client then uses this capability to request the document from server 2 as described in a precedent section.

A limitation of this method is that each time a node migrates, the retrieval protocol is increased by the first three protocol steps. This is not practical when nodes migrate frequently from one server to another. Another limitation is an increase of the trust placed on content servers: content servers can now grant access to other content servers.

4.2 Use of Uniform Resource Names (URNs)

A URN is a logical reference to a node. *Name servers* provide a resolution of URNs into URLs. This scheme can be integrated into the model by defining a *URN capability* type that, instead of granting access to a node, grants access not only to a node's URL but also to an appropriate capability for requesting that node. Document servers now store URN capabilities along with documents. Name server store node capabilities along with the URLs.

The protocol is as follows (Table 8):

1 and 2. A client requests a protected document from the document server.

3. The document server returns a delegated list of URN capabilities and the document.

4 and 5. Before retrieving a document, the client

1. Client to Document Server: Authentication according to the GIA
2. Client to Document Server: Request-Document + DDcap
3. Document Server to Client: Response-Document + {DURNDcap} + {DURNCcap}
4. Client to Name Server: Authentication according to the GIA
5. Client to Name Server: URN of Document + DURNDcap
6. Name Server to Client: URL of Document + DDcap

Table 8: URN support

contacts the name server to find the document's URL. As with a node request, the client must authenticate itself to the name server and present an appropriate capability.

6. Having authorized the request, the name server returns the URL and a delegated version of the corresponding capability.

A limitation of this method is that both content and name servers must be trusted as they can grant access to other servers. Note that with this method, a client always executes the same number of protocol steps to retrieve a node, regardless of how many times the node has migrated.

5 A group extension

The group extension supports non-sequential access to nodes. Figure 2 shows the modifications to the authorization model.

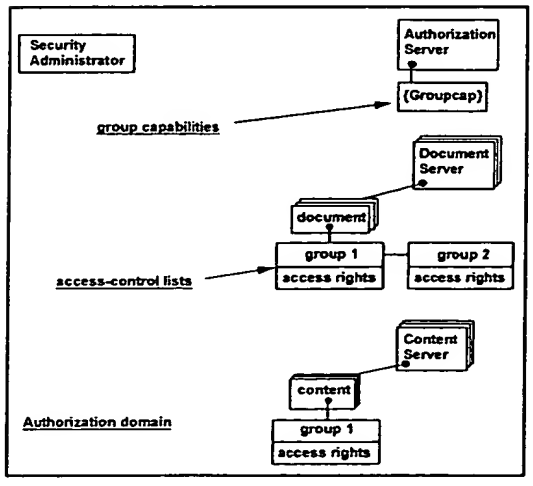


Figure 2: Group support overview

In this extension, each node is associated with an ACL. Each entry of the ACL is a double-tuple which includes a group name and the access rights that the group has over the node. Group names correspond to presentation trees. Thus, all the nodes used in a presentation tree have the same group entry. On the other hand, the entries of a node's ACL correspond to all the presentation trees that use that node. In order to retrieve any of the nodes used in a presentation tree, a client needs to join a *group capability* (Groupcap) to its node requests. A group capability, which is granted by the AUS, gives a client access to a presentation tree for a given time. The format of this capability is the same as the one shown in Table 1, but includes a group name instead of a node identifier.

1. Client to AUS: Group Name + [authorization info]
2. AUS to Client: DGroupcap
3. Client to Node Server: Authentication according to the GIA
4. Client to Node Server: Node URL + DGroupcap
5. Node Server to Client: Node

Table 9: Group extension protocol

The message exchanges for this protocol are similar to those described in Section 3.4 (Table 9). Document servers do not have to delegate capabilities as the client only needs one group capability to access any node of the tree. To authorize a node request, node servers not only have to validate the capabilities, but they also have to validate the capability and the request against the node's ACL. The group extension is independent of node migration techniques as it merely requires that a migrating node's ACL migrate too.

We shall now discuss how this extension affects the limitations of our model. As a document server no longer delegates capabilities, the compromise of such a server does not affect other node servers. This authorization method is faster than the preceding one as it only requires one delegation operation. A client wishing to follow a bookmark link to a document still needs an appropriate capability. Once the capability expires, the client just needs to acquire a new group capability to reuse the bookmark link. This authorization scheme still requires the evaluation of the client consultation time for a presentation tree. Node migration support does not place any additional trust in content servers or name servers.

The principal limitation of this extension is that each presentation tree needs to have a unique identifier. Another limitation is that the inclusion of an existing node into a presentation tree requires the updating of the node's ACL. Finally, searching a node's ACL may be cumbersome if the node is a component of several presentation trees.

6 Implementation considerations

This section describes the principal choices and problems we have encountered while implementing the model. [9] describes the implementation in further detail.

In order to validate the concepts of the model, we have developed a prototype of the model which includes the node redirection support and the group extension. We chose to build the prototype on NCSA's WWW client (Mosaic 2.4) and server (httpd 2.3) as this system proposes hooks to a PGP/PEM enciphering layer [16]. We used these hooks to "plug-in" an authorization layer to the system. This allowed us to quickly arrive at a working prototype.

The prototype uses the technique described in [15] to implement self-authenticating capabilities. Asymmetric keys are used to sign capabilities as well as to authenticate the grantor servers. The AUS's and SA's public keys are distributed to the node servers during the installation phase. The public keys of grantor servers are used as the value of the capabilities' *grantor server identifier* attribute, and are thus distributed inside the capabilities. Grantor servers use their private keys to sign the capabilities which they delegate as proof of their identity. Thus, each delegated capability contains the signature of a grantor server and the public key which allows to verify the signature.

A similar technique is used to authenticate clients. Clients uses their private keys to sign every request they make. When a client requests a capability from the AUS, the client includes in the request its identity and the root document's URL. In order to authenticate the client, the AUS must retrieve the client's public key from a local file or from a key certification center. Having authorized the request, the AUS creates an authorizator using the the client's public key as the value of the GIA. As the client's public key is distributed inside the authorizator, node servers can authenticate the client without having to contact other servers.

The above technique can be modified to minimize the use of a client's public key. In this variation, the AUS creates a session asymmetric key pair and uses the session public key as the value of the GIA. The AUS first enciphers the session private key using the client's public key and then sends it together with the delegated capability to the client. Thereafter, the client uses the session private key to sign its requests. The session key pair remains valid during the lifetime of the authorizator.

To exchange capabilities between clients and servers, we added a header to the HTTP messages. The drawback of this method is that the client had to be modified so that it could add and remove capabilities to and from messages. [3] proposes an alternative method whereby capabilities are exchanged inside documents. In this method, document servers embed each of a document's delegated node capabilities into their corresponding node's URLs before returning the requested document. The advantage of this method is that clients do not need to be modified: clients use augmented URLs in the same way as they use normal URLs. The drawback of this method is that document servers must parse each requested document.

A problem we have come across with the implementation of the group extension is that clients acquiring more than one group capability cannot tell which one they must use. As the implementation effectuates all authorization exchanges on the HTTP level, the documents do not provide any hint as to what group capability a client should present when following a link. As a consequence, clients have to try their group capabilities one after another until they score a hit. A solution to this problem is to have node servers return unauthorized messages which list all the group names associated with a node. This solution is not practical because popular nodes may be used in several presentation trees. Moreover, clients have to waste a transaction to find out which capability they must use. Another solution is to modify the client so that it remembers which group capability it used when it successfully followed a link. In this way, the client can use the same group capability when following other related links.

7 Related work

This section briefly mentions related work that has been done in the area of coordinated WWW distributed authorization.

DCE Web [13, 14] is an on-going project to marry OSF's Distributed Computing Environment with WWW. DCE Web adds to WWW the advantages of DCE security, which include distributed authentication, consistent group[2] ad-

[2] In DCE, a group is a list of clients who share a set of access rights to a set of objects or services.

ministration across a domain, protection of nodes with ACLs, and remote administration of ACLs. Client authentication is implemented using a conventional key trusted third party scheme derived from Kerberos [22]. Rather than having each server define its own groups, groups are handled by the same third party which handles user authentication. The authentication credentials, which a user retrieves to contact a server, include the user's group attributes. Although DCE Web does not explicitly support coordinated authorization for distributed documents and contents, it provides several tools that can be used to reach that goal. For example, DCE Web's group support can be used to implement our model's group extension using a conventional key cryptosystem.

The Phoenix project [12] is a distributed hypermedia authoring system which integrates access control information to hypermedia documents. Documents are protected by means of ACLs; however, instead of storing the documents together with the ACLs, each document includes an HTML mark-up element giving the URL of an ACL. To authorize document requests, a document server sends the requested method, the ACL URL reference, and the authenticated client-name to an authorization server. The authorization server retrieves the ACL, searches it for an adequate entry, and returns the authorization result to the document server. Authorized users can change both the ACL and the links that point to it in a remote fashion. Phoenix can support coordinated authorization by having different documents share the same ACL. We were not able to find out how Phoenix protects contents or other non-html objects. Compared with Phoenix, our model protects documents without needing to modify them. Authorization in our model is handled locally by each node server whereas Phoenix uses a centralized authorization server. In our model as well as in Phoenix, only one server needs to know its potential clients.

Hyper-G [10, 2] is a second-generation, large-scale distributed hypermedia system which uses an object-oriented database layer to provide, among other features, information-structuring and link-maintenance facilities, as well as a hierarchical access control scheme. Contents are stored outside of the database. Access can be restricted to contents[3], documents, and presentation trees to certain groups of users. Hyper-G also supports the modification of the database by authorized clients. A Hyper-G system comprises a link server and a collection of content servers. The link server is responsible for handling the database and authorizing the client requests. In a typical session, a client authenticates itself to a link server and then sends its node requests to it. Requests can be either for information contained in the database or for contents. In the latter case, it is the link server, and not the client, which contacts the content server and instructs it to send the contents to the client. Both our model and Hyper-G provide authorization at both the presentation tree and document levels. Hyper-G's use of a centralized server allows it to provide even a finer level of authorization granularity. Moreover, the use of a centralized server provides a practical client and database administration. Our model uses a distributed authorization approach. Although our model simplifies client administration, it presents problems when trying to revoke capabilities before their validation period expires. In both models, only one server needs to know its potential clients.

Sessioneer [3] is a recently proposed framework which is close to our authorization model. Sessioneer uses certificates (similar to capabilities) to control access to documents. Clients authenticate once when retrieving a root document. Document servers parse each requested document and embed certificates into the document's outgoing node links. Clients automatically use those certificates when traversing a link. Although some possible attributes of certificates are cited, such as the client's identity, client's IP address, and time stamps, Sessioneer leaves the definition of a certificate format to the applications. This model does not require any modification of clients nor servers. As in our model, user annotations have a limited life. Our model defines a more specific capability format in order to reach the goal of distributed authorization. It should be possible to combine both approaches in order to enjoy the advantages of each.

8 Concluding remarks

We believe that supporting coordinated authorization for distributed documents and contents is an important issue for WWW systems as it will not be always possible to store everything in a single server. By storing nodes according to their types into specialized servers, the overall workload of the system will be better balanced.

We have presented an authorization model that provides coordinated, distributed authorization at the presentation tree and document levels. The use of capabilities as an access-control mechanism simplifies the administration of clients

[3] Hyper-G documents use the term *document* to refer to contents and the term *collection* to refer to either a document or a presentation tree. In order to have a homogeneous terminology, we converted their notation into the one used in this paper.

and distributes the authorization process among different node servers. The model provides both sequential- and non-sequential access modes. The model supports existing WWW node migration techniques. We also explained choices we have made and problems we have encountered while building a prototype of the model. Some solutions to those problems were also proposed.

We believe that our authorization model can be used to protect access to persistent presentation trees when the client population changes at a fast rate; for example, an electronic public library where a client buys access for a limited period.

Other authorization approaches use centralized authorization servers which are consulted each time a client requests a node. A deeper comparison of both distributed and centralized authorization approaches is necessary to know in what situations each one might be better used.

Acknowledgments

The author sincerely thanks the Program Committee of INET'95 for their financial support for publishing and presenting this paper. This work was financed by a grant from CONACyT, a Mexican public institution, and the CCETT, a France Telecom joint research center for broadcast and telecommunications.

References

[1] S. G. Akl, "Digital Signatures: A Survey," tech. report 82-145, Department of Computing and Information Science, Queen's University, Kingston, Ontario, Canada, Now, 1982.

[2] K. Andrews, F. Kappe, and H. Maurer, "Serving Information on the Web with Hyper-G," in *Proc. Third World-Wide Web Conference*, pp. 919-926, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/105/hgw3.html

[3] S. Anderson and R. Garvin, "Sessioneer: Flexible Session Level Authentication with off the Shelf Servers and Clients," In *Proc. Third World-Wide Web Conference*, pp. 1047-1053, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/77/sessioneer2.html

[4] T. Berners-Lee, Hypertext Transfer Protocol, Internet Draft, 5 Nov. 1993 (Expires 5 May 1994).

[5] T. Berners-Lee, Uniform Resource Locators - A unifying syntax for the expression of names and addresses of objects on the network, Internet draft, draft-ietf-uri-url-02.ps. 1 Jan. 1994, expires 1 Jul. 1994.

[6] T. Berners-Lee, R. Cailliau, A. Luotonen, H. Frystik Nielsen, and A. Secret, "The World-Wide Web," Comm. of the ACM, Vol. 37, No. 8, pp. 76-82, Aug. 1994.

[7] European Computer Manufacturers Association, Standard ECMA38: Security in Open Systems - Data Elements and Service Definitions, ECMA, Dec. 1989.

[8] J. Kahan, "Un nouveau modèle d'autorisation pour les systèmes de consultation d'information multimédia répartie," In *Proc. Où, quand, commment protéger vos logiciels et documents électroniques*, AFCET, Dec. 1994. (In French)

[9] J. Kahan, "A Capability-Based Authorization Model for the World-Wide Web," In Proc. *Third World-Wide Web Conference*, pp. 1055-1064, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/86/CAMWWW.html

[10] F. Kappe, Hyper-G Technical Documentation. http://info.iicm.tu-graz.ac.at/Ctechnical

[11] K.-Y. Lam and D. Gollman, "Freshness Assurance of Authentication Protocols," In Proc. *ESORICS 92*, pp. 293-303, 1992.

[12] M. G. Lavenant and J. A. Kruper, "The Phoenix Project:Distributed Hypermedia Authoring," In *Proc. First World-Wide Web Conference*, Spring 1994. http://www.cern.ch/PapersWWW94/j-kruper.ps

[13] S. Lewontin and M. E. Zurko, "The DCE Web Project: Providing Authorization and other Distributed Services to the World-Wide Web," In *Proc. Second World-Wide Web Conference*, 1994. http://www.ncsa.uiuc.edu/SDG/IT94/Proceedings/Security/

[14] S. Lewontin, "The DCE Web Toolkit: Enhancing WWW Protocols with Lower-Layer Services," In *Proc. Third World-Wide Web Conference*, pp. 765-771, Apr. 1995.// http://www.igd.fhg.de/www/www95/papers/67/DCEWebKit.html

[15] M. R. Low and B. Christianson, "Technique for Authentication, Access Control and Re-

source Management in Open Distributed Systems," Electronic Letters, Vol. 30, No. 2, pp. 124-125, 20 Jan. 1994.

[16] R. McCool, Using PGP/PEM Encryption. http://hoohoo.ncsa.uiuc.edu/docs/PEMPGP.html

[17] B. Clifford Neuman, "Proxy-Based Authorization and Accounting for Distributed Systems," In *Proc. 13th Int. Conf. on Dist. Comp. Syst.*, Pittsburgh, pp. 283-291, May 1993.

[18] K. E. Rowe and C. K. Nicholas, "Reliability of WWW name servers," In *Proc. Third World-Wide Web Conference*, pp. 773-783, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/75/rowe_release_2/www-reliable.html

[19] R. S. Sandhu and P. Samarati, ' Access Control: Principles and Practice," IEEE Comm. Magazine, pp. 40-48, Sep. 1994.

[20] J.H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," Proc.of the IEEE, 63(9), pp. 1278-1308, 1975.

[21] K. Sollins and L. Masinter, Functional Requirements for Uniform Resource Names, draft-ietf-uri-urn-req-01.txt, 14 Oct. 1994.

[22] J. G. Steiner, C. Neuman, and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," In *Proc. Winter USENIX Conf.*, 1988.

[23] V. Varadharajan, P. Allen, and S. Black, "An Analysis of the Proxy Problem in Distributed Systems," In *Proc. IEEE Symp. on Security and Privacy*, pp. 255-275, 1991.

[24] M. E. Zurko and P. M. Hallam-Baker, "Secure Authorization Issues on the Web," In *Tutorial Notes - Third World-Wide Web Conference*, pp. 143-186, Apr., 1995.

Author Information

José Kahan is a PhD candidate in Computer Science at the Université de Rennes I (France). He is working on authorization issues and models for distributed hypermedia consultation services. He holds a specialization degree in Computer Networks from the Ecole Supérieure d'Electricité (France), and a degree in Electronics Engineering from the Universidad Autonoma Metropolitana-Azcapotzalco (Mexico).

Author contact (expires October 1995):

CCETT AMS/ARM
4, rue du Clos-Courtel BP 59
35512 CESSON-SEVIGNE CEDEX
FRANCE

[Help] *Last update at http://inet.nttam.com : Fri May 19 15:45:20 1995*

INET'95 Hypermedia Proceedings -- Author Information

Please update and improve your on-line paper

FTP server (ftp.nttam.com) for hypermedia proceedings is available for any correction and addtional materials.

Materials Specification

Contents	Preferable Format	FILENAME(example)
Revised paper	tar (HTML and GIF)	012.paper.tar[.Z]
	HTML	012.paper.html
	ASCII text	012.paper.txt
	GIF	012.graph1.gif
Your portrait	GIF,200x200 or less	012.picture.gif
Audio for abstract	AU	012.audio.au
Video clip	QuickTime	012.video.mov
		^^^
		XXX=3 digit Paper ID
		[Required]

If you can not create a file using data format above, please contact to inet-hmp-sec@nttam.com.

Directions to upload (in case of UNIX)

1. **ftp ftp.nttam.com**.
2. login in as **anonymous**, and enter **your email address** as password
3. **cd post** (move to directory for posting)
4. **binary** (when sending a binary file)
5. **put FILENAME**
6. **quit**

Please do not forget that you cannot overwrite a file of the same name. So at the second time, you may send a file with different name. After uploading a file, please send an email message to inet-hmp-sec@nttam.com.

Thank you.

inet95@nttam.com